# BULLETIN

OF THE

# AMERICAN MATHEMATICAL SOCIETY

EDITED BY

EARLE R. HEDRICK
DAVID R. CURTISS WILLIAM R. LONGLEY

WITH THE ASSISTANCE OF

HAROLD T. DAVIS HARRY W. KUHN
THEOPHIL H. HILDEBRANDT DERRICK N. LEHMER
JOHN R. KLINE HENRY L. RIETZ
CAROLINE E. SEELY

VOLUME XL, NUMBER 2

FEBRUARY, 1934

PUBLISHED BY THE SOCIETY
MENASHA, WIS., AND NEW YORK
1934

---

Whole No. 413 $9.00 a Year

PUBLISHED MONTHLY

Entered as second class matter April 24, 1926 at the post office at Menasha, Wis., under the act of August 24, 1912.

# AMERICAN MATHEMATICAL SOCIETY

**Mail Address:** 501 West 116th Street, New York, N.Y., for the Secretary, Treasurer, Librarian, and Clerk.

**Office:** Room 413, Physics Building, Columbia University, New York City.

**President:** Professor A. B. Coble, University of Illinois, Urbana, Ill.

**Secretary:** Dean R. G. D. Richardson, Brown University, Providence, R.I.

**Associate Secretaries:** Professor M. H. Ingraham, University of Wisconsin, Madison, Wis.; Professor J. R. Kline, University of Pennsylvania, Philadelphia, Pa.; Dean T. M. Putnam, University of California, Berkeley, Calif.

**Treasurer:** Professor G. W. Mullins, Barnard College in Columbia University, New York City.

**Librarian:** Professor R. C. Archibald, Brown University, Providence, R.I.

**Clerk:** Dr. Caroline E. Seely, 413 Physics Building, Columbia University, New York City.

**Editor-in-Chief of the Bulletin:** Professor E. R. Hedrick, University of California at Los Angeles, Los Angeles, Calif.

**Managing Editor of the Transactions:** Professor R. D. Carmichael, University of Illinois, Urbana, Ill.

Chairman, Colloquium Editorial Committee: Professor Oswald Veblen, The Institute for Advanced Study, Princeton, N.J.

**Managing Editor of the American Journal of Mathematics:** Professor Abraham Cohen, Johns Hopkins University, Baltimore, Md.

**Representatives of the Society in the Division of Physical Sciences of the National Research Council:** Professors A. B. Coble, E. R. Hedrick, and Dean R. G. D. Richardson.

**Representatives on the Council of the American Association for the Advancement of Science:** Professors M. H. Ingraham and C. N. Moore.

**Chairman, Committee on Arrangements for the Semi-Centennial:** Professor T. S. Fiske, Columbia University, New York City.

# NOTE ON A PROBLEM OF FRÉCHET*

BY ROTHWELL STEPHENS

1. *Introduction.* Fréchet has proposed the following problem: Characterize the most general space in which there exists a non-constant real-valued continuous function. Its solution has been given by Urysohn† for the spaces of Hausdorff and by Chittenden‡ for topological spaces.

However, in his generalization, Chittenden used for his definition of a continuous function a neighborhood definition§ of Fréchet which is not entirely adequate for the general topological space. That the definition is not adequate is easily shown by the following example. Let the space $(P, K)$ be a set of points corresponding to the open interval $[0, 1]$. For any set $E$ of $(P, K)$, $K(E)=R(E)+J(E)$. A point $x$ is in $R(E)$ if $x$ is in a derived set of $E$ under the metric relationship. A point $x$ is in $J(E)$ if $E$ contains both $x$ and the open interval $[0, x/2]$. A neighborhood of $x$ is any set to which $x$ is interior. The correspondence $f(x)=x$ between the space $(P, K)$ and the space $(P, R)$ determines under the Fréchet definition a biunivocal bicontinuous transformation, although the two spaces are not homeomorphic.

The purpose of this paper is to solve the problem for the general topological space using the Sierpinski definition‖ of a continuous transformation. The notation used will be that of Chittenden.¶

2. *Thoroughly Interior.* A point $a$ is said to be *thoroughly in-*

---

* Presented to the Society, July 18, 1933..

† Urysohn, *Über de Mächtigkeit der zusammenhängenden Mengen*, Mathematische Annalen, vol. 94 (1925), p. 290.

‡ Chittenden, *On general topology and the relation of the properties of the class of all continuous functions to the properties of space*, Transactions of this Society, vol. 31 (1929), p. 310.

§ Chittenden, loc. cit., p. 309.

‖ Sierpinski, *La notion de dérivée comme base d'une théorie des ensembles abstraits*, Mathematische Annalen, vol. 97 (1926), pp. 321–337.

¶ Chittenden, loc. cit. Also see Stephens, *Continuous transformations of abstract spaces*, Transactions of this Society, vol. 34 (1932), p. 395.

*terior* to a set $E$ if $a$ is contained in $E$ and not contained in $L[C(E)+a]$.* A set $A$ is thoroughly interior to a set $E$ if each point of $A$ is thoroughly interior to $E$. A set $E$ is thoroughly open if each point of $E$ is thoroughly interior to $E$. The complement of a thoroughly open set we shall call a thoroughly closed set. It is easily seen that in a neighborhood space every open (closed) set is thoroughly open (closed). Furthermore the sum of an infinite number of thoroughly open (closed) sets is thoroughly open (closed).

THEOREM 1. *If $f$ is a continuous transformation such that $f(P)=Q$, and $b$ is a point thoroughly interior to $B \subset Q$, then $g(b)$ is thoroughly interior to $g(B)$.*†

The proof is by contradiction. Assume $g(b)$ is not thoroughly interior to $g(B)$. Then there exists a point $a$ of $g(b)$ and a set $E \subset C[g(B)]$ such that $a \subset (E+a)'$ but not in $E'$ since $g(b)$ is interior to $g(B)$.‡ Then $f(a) \subset f(E)+[f(E+a)]' \subset [f(E-a)]$, which is impossible.

As a corollary we have the following theorem.

THEOREM 2. *A necessary condition that a transformation be continuous is that the inverse of every thoroughly open (closed) set be thoroughly open (closed).*

THEOREM 3. *If a space $(P, K)$ has no singular points,§ then there exists a V-space $(P, W)$ which is a biunivocal continuous transformation of $P$ in such a way that thoroughly open (closed) sets are transformed into open (completely closed) sets.*

The space $(P, W)$ is defined on the set $P$ as follows. For each point $a$ of $P$, if $a \subset K(E)$ in $(P, K)$, then $a \subset W(B)$ in $(P, W)$, where $B$ is any set containing $(E-a)$. The space $(P, W)$ is a neighborhood space which is the biunivocal continuous transform of $(P, K)$ under the transformation $f$ which carries each point into itself.‖ Furthermore, if any set $O$ is thoroughly $K$-

* $L(E)$ is the set of all $K$-points of all subsets of $E$. Chittenden, loc. cit., p. 294. $C(E)$ is the complement of $E$ in $P$.

† By $g(b)$ is denoted the set of all points of $P$ to which $b$ of $Q$ corresponds under $f$.

‡ Stephens, loc. cit., p. 397.

§ A point is a singular point if $a \subset K(a)$. Stephens, loc. cit., p. 396.

‖ Stephens, loc. cit., p. 405.

open, it is thoroughly $W$-open. For suppose $O$ is thoroughly $K$-open but not thoroughly $W$-open. Then there exists a point $a$ of $O$ such that $a \subset W(B)$ where $B \subset C(O)$. Hence $a \subset K(E)$ where $(E-a) \subset B \subset C(O)$, and $O$ cannot be thoroughly $K$-open, contrary to hypothesis. The proof for thoroughly closed sets is obvious.

3. *Normal Families of Thoroughly Open Sets.* A family of thoroughly open sets $G$ is normal† provided

(a) there exist two sets $G_0$, $G_1$ of the family which are distinct and such that $G_0 \subset G_1$;

(b) if $G_0$, $G_1$ are any two sets of the family such that $G_0^* \subset G_1$,‡ there is a set $G$ such that

$$G_0^* \subset G \subset G^* \subset G_1.$$

THEOREM 4. *If the continuous transform $Q$ of a space $P$ contains a normal family of thoroughly open sets, then the original space $P$ contains such a family.*

Since $G_0 \subset G_1$ are thoroughly open sets, $g(G_0) \subset g(G_1)$ are thoroughly open sets satisfying condition (a). For the inverse sets of

$$G_0^* \subset G \subset G^* \subset G_1$$

we have the relation

$$g(G_0^*) \subset g(G) \subset g(G^*) \subset g(G_1),$$

where $g(G_0^*)$ and $g(G^*)$ are thoroughly closed sets. We have then§

$$g(G_0) \subset [g(G_0)]^* \subset g(G_0^*) \subset g(G) \subset [g(G)]^* \subset g(G^*) \subset g(G_1).$$

Hence $P$ contains a normal family of thoroughly open sets.

THEOREM 5. *If a space $P$ contains no singular points and possesses a normal family of thoroughly open sets, there exists a V-space $Q$ having a normal family of open sets, which is a biunivocal continuous transform of $P$.*

By Theorem 3, there is a space which is a biunivocal continuous transform $Q$ of $P$ such that thoroughly open (closed) sets

† Chittenden, loc. cit., p. 310.

‡ The set $G_0^*$ is the least thoroughly closed set containing $G_0$.

§ $g(G_0)^* \subset g(G_0^*)$ since the product of a finite or infinite family of thoroughly closed sets is thoroughly closed.

are transformed into open (completely closed) sets. It remains to show that $Q$ contains a normal family of open sets.

Let $G$ be the normal family of thoroughly open sets in $P$. Then $f(G_0)$ and $f(G_1)$ satisfy condition (a). Also $f(G_0) \subset f(G_0^*) \subset f(G) \subset f(G^*) \subset f(G_1)$, from which we have

$$f(G_0) \subset [f(G_0)]^* \subset f(G) \subset [f(G)]^* \subset f(G_1).$$

Hence $Q$ possesses a normal family of open sets and the theorem is proved.

4. *Non-Constant Continuous Functions.* We are now prepared to prove the following generalization of the Urysohn theorem.

THEOREM 6. *A necessary and sufficient condition that a topological space admit the existence of a non-constant real-valued continuous function is that it contain a normal family of thoroughly open sets and that it contain no singular points.*

The necessity of the normality requirement is immediate from Theorem 4. I† have proved that the space $P$ must contain no singular point.

To prove that the conditions are sufficient we use Theorem 5 to obtain a $V$-space possessing a normal family of open sets. But now the Fréchet definition holds and the theorem of Chittenden‡ is valid.

It should be noted that the requirement of normality is significant only in connected spaces. The Urysohn corollary to this theorem as stated by Chittenden§ holds.

KNOX COLLEGE

† Stephens, loc. cit., p. 405.
‡ Chittenden, loc. cit., p. 310.
§ Chittenden, loc. cit., p. 310.

# ON THE SUMMATION OF FOURIER SERIES

BY R. E. A. C. PALEY, W. C. RANDELS, AND M. F. ROSSKOPF

1. *Introduction.* Suppose that we have a series

$$u_1 + u_2 + u_3 + \cdots \tag{1}$$

and an infinite matrix $\{\eta_{n,m}\}$, $(0 \leqq n < \infty,\ 1 \leqq m < \infty)$. We say that the series is summable by the method $\{\eta\}$, if the sum

$$\sum_{n=0}^{\infty} u_n \eta_{n,m} \tag{2}$$

tends to a limit as $m$ tends to infinity.

The method $\{\eta\}$ is said to be regular if, whenever (1) is convergent, (2) tends to the same limit.

Hille and Tamarkin* call a method of summability $F$-effective, if it sums the Fourier series of an integrable function to the value of the function at every point $x$ where the function has a definite value $f(x)$ and where

$$\phi(t) \equiv f(x+t) + f(x-t) - 2f(x) = o(1),$$

as $t \to 0$. They call a method $L$-effective if it sums the Fourier series of an integrable function to the value of the function at every point of the Lebesgue set of the function; that is, at every point $x$ where

$$\int_0^h |\phi(t)|\, dt = o(h).$$

The object of this paper is to construct a method of summation which is regular and $F$-effective without being $L$-effective.†

2. *Outline of the Method.* We restrict ourselves to methods of

* E. Hille and J. D. Tamarkin, *On the summability of Fourier series*, Transactions of this Society, vol. 34 (1932), pp. 757–783.

† This problem was proposed to the late R. E. A. C. Paley by Professors Hille and Tamarkin. Before his death, Paley had worked on the problem, leaving an unfinished and incomplete manuscript. On the basis of his work Randels and Rosskopf have proceeded and have been able to solve the problem.

summation where $\eta_{n,m}$ is of the form $\eta(n/m)$; so that (2) becomes

$$\sum_{n=0}^{\infty} u_n \eta(n/m). \tag{3}$$

The function $\eta$ need only be defined for rational values of the argument, but it is simpler to suppose that it is defined for all values of $x$ from zero to infinity. We shall suppose that (a) $\eta(x)$ is of bounded variation over $(0, \infty)$, and that $\eta(0) = \eta(+0) = 1$. It can easily be shown that the conditions (a) imply the regularity of the method of summation $\{\eta\}$.

Suppose that ($b_1$) $\eta(x) \to 0$ as $x \to \infty$. Then the cosine Fourier transform

$$K(t) = \left(\frac{2}{\pi}\right)^{1/2} \int_0^{\infty} \eta(x) \cos tx \, dx \tag{4}$$

must exist, and the integral (4) must converge as an improper integral. Suppose further that ($b_2$)

$$\int_0^{\infty} |K(t)| \, dt < \infty. \tag{5}$$

Hille and Tamarkin* have shown that the existence of the integral (5) is necessary and sufficient in order that a method of summation which satisfies (a) and ($b_1$) be $F$-effective.

The outline of our method is as follows. We construct a kernel $K(t)$ which furnishes a method of summability which is $F$-effective. Then we construct a particular function $f(x)$, $f(0) = 0$, the point $x = 0$ belonging to the Lebesgue set of $f(x)$, such that the method $\{\eta\}$ does not sum the Fourier series of $f(x)$ to zero at $x = 0$.

3. *Construction of the Kernel.* The kernel which we shall use is defined by

$$K(t) = \sum_{n=1}^{\infty} K_n(t),$$

* In an unpublished paper presented to the Society; see E. Hille and J. D. Tamarkin, *On the summability of Fourier series*, IV, this Bulletin, vol. 39, Abstract 181, May (1933).

where

$$K_n(t) = \begin{cases} +\dfrac{1}{tn^{3/2}}(t - 2^n + n^{1/2}), & 2^n - n^{1/2} \leqq t \leqq 2^n, \\ -\dfrac{1}{tn^{3/2}}(t - 2^n - n^{1/2}), & 2^n \leqq t \leqq 2^n + n^{1/2}, \\ 0, & \text{elsewhere}, \end{cases}$$

for $n = 1, 2, \cdots$. Then it can easily be proved that

$$K(t) \subset L, \qquad K^*(t) \equiv tK(t) \subset L_2,$$

and that $K(t)$ is of bounded variation over $(0, \infty)$. We define $A$ by

$$A = \left(\left(\frac{2}{\pi}\right)^{1/2} \int_0^\infty K(t)dt\right)^{-1}.$$

Let us define $\eta(x)$ as

$$\eta(x) = A\left(\frac{2}{\pi}\right)^{1/2} \int_0^\infty K(t) \cos tx \, dt;$$

then $\eta(0) = 1$. Now we consider the Fourier series of an even, integrable, periodic function $f(x)$,

$$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos nx;$$

then if we replace $x$ by $t/m$, multiply the Fourier series of $f(t/m)$ by $A(2/\pi)^{1/2} K(t)$, and integrate from zero to infinity, we obtain

$$\begin{aligned} A\left(\frac{2}{\pi}\right)^{1/2} \int_0^\infty K(t)f(t/m)dt &= A\,\frac{a_0}{2}\left(\frac{2}{\pi}\right)^{1/2} \int_0^\infty K(t)dt \\ &+ A\left(\frac{2}{\pi}\right)^{1/2} \int_0^\infty K(t)\left(\sum_{n=1}^{\infty} a_n \cos\frac{n}{m}t\right)dt \\ &= \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \eta(n/m). \end{aligned} \tag{6}$$

This step is legitimate since $K(t)$ is of bounded variation over $(0, \infty)$.†

By Plancherel's theorem for Fourier integrals, since $K^*(t) \subset L_2$, we have

$$\eta_0^*(x) \sim A\left(\frac{2}{\pi}\right)^{1/2} \int_0^\infty K^*(t) \sin xt\, dt \subset L_2$$

over $(0, \infty)$. Furthermore if we denote by $\eta_n^*(x)$ the Fourier transform of $K_n^*(x)$, we can write

$$\eta^*(x) = \sum_{n=1}^{\infty} \eta_n^*(x) = A \sum_{n=1}^{\infty} \int_{2^n - n^{1/2}}^{2^n + n^{1/2}} K_n^*(t) \sin xt\, dt$$

$$= A \sum_{n=1}^{\infty} \frac{2 \sin 2^n x (1 - \cos n^{1/2} x)}{x^2 n^{3/2}}. \tag{7}$$

It is easily seen that $\eta^*(x)$ exists everywhere; hence $\eta_0^*(x) = \eta^*(x)$ almost everywhere. Now clearly $\eta^*(x)$ is integrable over $(a, \infty)$, $a > 0$, and $\eta_0^*(x)$ is integrable over the interval $(0, a)$; hence $\eta^*(x) \subset L$ over the interval $(0, \infty)$. We write

$$\int_0^x \eta^*(u)du = \lim_{\delta \to 0} \int_\delta^x \left\{ \sum_{n=1}^{\infty} \eta_n^*(u) \right\} du. \tag{8}$$

The sum (7) is dominated by

$$A \sum_{n=1}^{\infty} \frac{1}{x^2 n^{3/2}},$$

which belongs to $L$ over $(\delta, x)$; hence we may integrate (8) termwise; this gives

$$\int_0^x \eta^*(u)du = \lim_{\delta \to 0} \sum_{n=1}^{\infty} A \int_\delta^x du \int_0^\infty K_n^*(t) \sin ut\, dt.$$

Since $K_n^*(t)$ vanishes except on a finite interval, we may interchange the order of integration and obtain

† See E. V. Hobson, *The Theory of Functions of a Real Variable and the Theory of Fourier's Series*, 2d edition, 1926, vol. II, p. 583. Also G. H. Hardy, *Notes on some points in the integral calculus*, LV, Messenger of Mathematics, vol. 51 (1922), pp. 186–192.

$$
\begin{aligned}
\int_0^x \eta^*(u)du &= \lim_{\delta\to 0} \sum_{n=1}^{\infty} A \int_0^{\infty} K_n^*(t) \frac{\cos \delta t - \cos xt}{t} dt \\
&= \lim_{\delta\to 0} \sum_{n=1}^{\infty} A \int_0^{\infty} K_n(t)(\cos \delta t - \cos xt)dt \\
&= \lim_{\delta\to 0} A \int_0^{\infty} K(t)(\cos \delta t - \cos xt)dt \\
&= A \int_0^{\infty} K(t)dt - \eta(x),
\end{aligned}
\tag{9}
$$

since $K(t)$ is integrable. Consequently the right-hand member of (9), as an indefinite integral of an integrable function, is of bounded variation; hence $\eta(x)$ must be of bounded variation. Furthermore, $\eta(x)\to 0$ as $x\to\infty$, since it is the Fourier transform of an absolutely integrable function.

Therefore the method of summability defined by $\eta(x)$ is regular and $F$-effective.

4. *Construction of the Function.* However, this method is not $L$-effective. For consider the even periodic function

$$
f(x) = \begin{cases} 2^n, 2^{-n} - \dfrac{4^{-n}}{2\log(n+1)} \leqq x \leqq 2^{-n} + \dfrac{4^{-n}}{2\log(n+1)}, \\ 0, \text{ elsewhere in } (0, 2\pi), \end{cases}
$$

so that $f(0) = 0$.

Let us take for consideration the point $x = 0$. This point belongs to the Lebesgue set of $f(x)$ since

$$
\begin{aligned}
\int_0^t f(x)dx &= O\left( \sum_{n=[-\log_2 t]-1}^{\infty} \frac{2^{-n}}{\log(n+1)} \right) \\
&= O\left( \frac{2^{-[-\log_2 t]+2}}{\log([-\log_2 t])} \right) \\
&= O\left( \frac{t}{\log(-\log_2 t)} \right) = o(t),
\end{aligned}
$$

as $t\to 0$. At this point $x = 0$, then, the limit of (6) would have to be zero if the method were $L$-effective.

Consider the integral (6),

$$A\left(\frac{2}{\pi}\right)^{1/2}\int_0^{\infty}K(t)f(t/m)dt > A\left(\frac{2}{\pi}\right)^{1/2}\int_0^{m}K(t)f(t/m)dt.$$

Replace $m$ by $2^m$; then our function $f(x)$ becomes

$$f(t/2^m)=\begin{cases}2^n,\ 2^{m-n}-\dfrac{2^m4^{-n}}{2\log(n+1)}\leqq t\leqq 2^{m-n}+\dfrac{2^m4^{-n}}{2\log(n+1)},\\ 0,\ \text{elsewhere in } (0,2\pi), \qquad (n=1,2,3,\cdots).\end{cases}$$

Hence

$$A\left(\frac{2}{\pi}\right)^{1/2}\int_0^{2^m}K(t)f(t/2^m)dt > A\left(\frac{2}{\pi}\right)^{1/2}\sum_{n=1}^{[m/2]}\int_{J_n}K(t)f(t/2^m)dt,$$

where

$$J_n\equiv\left(2^n-\frac{2^m4^{n-m}}{2\log(m-n+1)},\ 2^n+\frac{2^m4^{n-m}}{2\log(m-n+1)}\right).$$

But over $J_n(n\leqq m/2)$, $K(t)>(1/4)(2^{-n}/n)$; therefore we have

$$\begin{aligned}&A\left(\frac{2}{\pi}\right)^{1/2}\sum_{n=1}^{[m/2]}\int_{J_n}K(t)f(t/2^m)dt\\ &\quad>A\left(\frac{2}{\pi}\right)^{1/2}\frac{1}{4}\sum_{n=1}^{[m/2]}\frac{2^{-n}}{n}\,\frac{2^m4^{n-m}}{\log(m-n+1)}\,2^{m-n}\\ &\quad=A\left(\frac{2}{\pi}\right)^{1/2}\frac{1}{4}\sum_{n=1}^{[m/2]}\frac{1}{n\log(m-n+1)}\\ &\quad>A\left(\frac{2}{\pi}\right)^{1/2}\frac{1}{4\log m}\sum_{n=1}^{[m/2]}\frac{1}{n}\sim A\left(\frac{2}{\pi}\right)^{1/2}\frac{1}{4},\end{aligned}$$

as $m\to\infty$.

Hence the method $\{\eta\}$ is not $L$-effective.

BROWN UNIVERSITY

# CURVATURES IN RIEMANNIAN SPACE*

BY HARRY LEVY

Let $C$ be a curve in Riemannian $n$-space with curvatures $1/\rho_\alpha$, $(\alpha=1, 2, \cdots, n-1)$. We shall designate by $\lambda_{1|}{}^i$, $(i=1, 2, \cdots, n)$ the components of the unit tangent vector and by $\lambda_{k|}{}^i$, $(i=1, 2, \cdots, n)$, those of the unit $(k-1)$st normal. Let $P$ and $P'$ be two points of $C$, and $\lambda^i$ and $\lambda'^i$ the components of two directions, one at $P$ and the other at $P'$. We shall speak of the *angle* between these directions, meaning the angle between $\lambda$ and the direction obtained at $P$ by parallel displacement along the curve of the direction $\lambda'$.† We denote by $\theta_k$ the angle, so defined, between the $(k-1)$st normals at $P$ and $P'$ (or, when $k=1$, between the tangents).

In euclidean three-space it is well known that

$$\lim \frac{\theta_1^2}{s^2} = \frac{1}{\rho_1^2}, \qquad \lim \frac{\theta_2^2}{s^2} = \frac{1}{\rho_2^2}, \qquad \lim \frac{\theta_2^2}{s^2} = \frac{1}{\rho_1^2} + \frac{1}{\rho_2^2},$$

where $s$ is the arc of $C$ from $P$ to $P'$. In fact, the curvatures are frequently defined by means of the first two of these equations. In extending the concept of curvature to a general Riemannian space this simple geometric interpretation was lost sight of, primarily because the earlier writers did not have available Levi-Civita's infinitesimal parallelism. As a consequence the curvatures, except the first, are usually defined by formal analytic methods. In this note we shall show that the above geometric interpretations of curvatures are valid in a general Riemannian space with a positive definite fundamental form. In the case of an indefinite form there is a very slight modification.

Let the curve $C$ be given parametrically by $x^i=x^i(s)$, $(i=1, 2, \cdots, n)$, where $s$ is the arc measured from an arbitrary point $P_0$. Let $g_{ij}$ be the components of the fundamental tensor and $\Gamma_{jk}^i$ the Christoffel symbols of the second kind, so that

* Presented to the Society, December 27, 1933.

† Since the angle between two directions at a point remains constant when the two directions are displaced parallel to themselves the above interpretation of the angle between two skew directions does not depend upon the order in which the two directions are taken.

$$\frac{\partial g_{ij}}{\partial x^k} = g_{jh}\Gamma^h_{ki} + g_{ih}\Gamma^h_{kj}. \tag{1}$$

We take for the $x$'s a system of normal coordinates with origin at $P_0$, so that

$$\left(\frac{\partial g_{ij}}{\partial x^k}\right)_0 = 0, \qquad (\Gamma^h_{ij})_0 = 0, \tag{2}$$

where the parenthesis with the subscript nought means that the expression within is evaluated at the origin $P_0$.

Following Eisenhart's notation‡ we can write the generalized Frenet equations

$$\lambda_{k|,j}{}^i \frac{dx^i}{ds} = -\frac{e_{k-1}}{\rho_{k-1}}\lambda_{k-1|}{}^i + \frac{e_{k+1}}{\rho_k}\lambda_{k+1|}{}^i, \tag{3}$$

where the $e$'s are $\pm 1$. Recalling the definition of covariant differentiation and making use of equations (2), we find that

$$\left(\frac{d\lambda_{k|}{}^i}{ds}\right)_0 = \left(-\frac{e_{k-1}}{\rho_{k-1}}\lambda_{k-1|}{}^i + \frac{e_{k+1}}{\rho_k}\lambda_{k+1|}{}^i\right)_0. \tag{4}$$

Differentiating equations (3) and eliminating the first derivatives of the $\lambda$'s by virtue of (3), we obtain the values of the second derivatives of the $\lambda$'s; at the origin they become, on account of (2),

$$\begin{aligned}\left(\frac{d^2\lambda_{k|}{}^i}{ds^2}\right)_0 = &\left(-\frac{\partial\Gamma^i_{hj}}{\partial x^l}\lambda_{k|}{}^h\frac{dx^i}{ds}\frac{dx^l}{ds} + \frac{e_{k-1}e_{k-2}}{\rho_{k-1}\rho_{k-2}}\lambda_{k-2|}{}^i\right)\\ &-\left(\frac{e_{k-1}}{\rho_{k-1}}\right)'\lambda_{k-1|}{}^i - e_k\left(\frac{e_{k-1}}{\rho^2_{k-1}} + \frac{e_{k-1}}{\rho^2_k}\right)\lambda_{k|}{}^i\\ &+\left(\frac{e_{k+1}}{\rho_{k+1}}\right)'\lambda_{k|}{}^i + \left(\frac{e_{k+1}e_{k+2}}{\rho_k\rho_{k+1}}\lambda_{k+2|}{}^i\right)_0,\end{aligned} \tag{5}$$

the primes in these equations denoting derivatives with respect to $s$.

---

* As usual an index appearing both as a subscript and a superscript is to be summed from 1 to $n$.

† See, for example, Eisenhart, *Riemannian Geometry*, p. 55.

‡ Loc. cit., p. 101.

The components $\lambda_{k|}{}^{i}$ of the $(k-1)$st normal at a point $P'$ near to $P_0$ are then given by the series expansions

$$\lambda_{k|}{}^{i} = (\lambda_{k|}{}^{i})_0 + \left(\frac{-e_{k-1}}{\rho_{k-1}}\lambda_{k-1|}{}^{i} + \frac{e_{k+1}}{\rho_k}\lambda_{k+1|}{}^{i}\right)_0 s + \tfrac{1}{2}Q_k{}^{i}s^2 + \cdots, \tag{6}$$

where with $Q_k{}^{i}$ we indicate the right hand sides of equations (5).

The unit direction of components $\mu^{i}=\mu^{i}(s)$ are parallel along $C$, in the sense of Levi-Civita,* if

$$\frac{d\mu^{i}}{ds} + \Gamma^{i}_{jk}\mu^{j}\frac{dx^{k}}{ds} = 0. \tag{7}$$

We obtain the values of successive derivatives of $\mu^{i}$ by differentiation, and, by making use of equations (2), we find that

$$\mu^{i} = (\mu^{i})_0 - \frac{1}{2}\left(\frac{\partial\Gamma^{i}_{jk}}{\partial x^{k}}\frac{dx^{j}}{ds}\frac{dx^{k}}{ds}\mu^{k}\right)_0 s^2 + \cdots.$$

In particular the components $\Lambda_{k|}{}^{i}$ of the vector at $P'$ parallel along $C$ to $\lambda_{k|}{}^{i}$ at $P_0$ are given by

$$\Lambda_{k|}{}^{i} = (\lambda_{k|}{}^{i})_0 - \frac{1}{2}\left(\frac{\partial\Gamma^{i}_{jk}}{\partial x^{l}}\lambda_{1|}{}^{j}\lambda_{1|}{}^{l}\lambda_{k|}{}^{k}\right)_0 s^2 + \cdots. \tag{8}$$

Finally, the series expansions of the $g$'s are given by

$$g_{ij} = (g_{ij})_0 + \frac{1}{2}\left(\frac{d^2g_{ij}}{ds^2}\right)_0 s^2 + \cdots, \tag{9}$$

where it is found by differentiation of

$$\frac{dg_{ij}}{ds} = (g_{jh}\Gamma^{h}_{li} + g_{ih}\Gamma^{h}_{lj})\frac{dx^{l}}{ds} \tag{10}$$

that

$$\left(\frac{d_2g_{ij}}{ds^2}\right)_0 = \left(\left\{g_{jh}\frac{\partial\Gamma^{h}_{li}}{\partial x^{k}} + g_{ih}\frac{\partial\Gamma^{h}_{lj}}{\partial x^{k}}\right\}\frac{dx^{k}}{ds}\frac{dx^{l}}{ds}\right)_0. \tag{11}$$

Since $\lambda_k$ and $\Lambda_k$ are unit vectors,

---

* See Eisenhart, loc. cit., p. 64.

$$\cos\theta_k = g_{ij}\lambda_{k|}{}^i\Lambda_{k|}{}^j, \tag{12}$$

where the quantities on the right are given by the power series (6), (8), and (9). Substituting these values and making use of the fact that the $\lambda$'s are mutually orthogonal unit vectors so that

$$g_{ij}\lambda_{k|}{}^i\lambda_{l|}{}^j = \begin{cases} 0 , & k \neq l, \\ e_k , & k = l, \end{cases} \tag{13}$$

we find

$$\cos\theta_k = e_k - \frac{1}{2}\left(\frac{e_{k-1}}{\rho_{k-1}^2} + \frac{e_{k+1}}{\rho_k^2}\right)_0 s^2 + \cdots . \tag{14}$$

Clearly*

$$\lim \frac{e_k - \cos\theta_k}{\theta_k^2} = \frac{1}{2}, \tag{15}$$

and consequently

$$\lim_{s\to 0} \frac{\theta_k^2}{s^2} = \frac{e_{k-1}}{\rho_{k-1}^2} + \frac{e_{k+1}}{\rho_k^2}. \tag{16}$$

In particular, since $1/\rho_0$ and $1/\rho_n$ are zero,

$$\lim \frac{\theta_1^2}{s^2} = \frac{e_2}{\rho_1^2}, \qquad \lim \frac{\theta_{n-1}^2}{s^2} = \frac{e_{n-1}}{\rho_{n-1}^2}. \tag{17}$$

If the fundamental form of the space is positive definite, the $e$'s are positive and the equations (16) are identical with the known relations in euclidean space.

THE UNIVERSITY OF ILLINOIS

---

* When the fundamental form is positive definite, the definition of $\theta_k$ and equations (15) present no difficulty. Otherwise $\cos\theta_k$ may be greater than one and $\cos\theta_k$ is not to be regarded as the cosine function of some number $\theta_k$ (see Eisenhart, loc. cit., p. 37). For our purpose it is sufficient to define $\theta_k$ as the complex number determined to within sign by $\theta_k^2 = e_k\{\cos^{-1}(e_k \cos\theta_k)\}^2$, where $\cos^{-1}$ is the principal value of the inverse cosine.

# A NOTE ON A CERTAIN PROPERTY OF A FAMILY OF CURVES

BY ALBERT WERTHEIMER

1. *Introduction.* In studying methods of constructing alignment charts for sets of empirical curves, it was found necessary to consider a certain property of the curves which we will call the closure property. Let $C_1$, $C_2$, and $C_3$ be three plane curves such that $C_2$ lies between $C_1$ and $C_3$; take any point $P$ on $C_2$ and make the following sequence of projections. Project $P$ vertically on $C_3$ into $P_3$, project $P_3$ horizontally on $C_1$ into $P_1$, project $P_1$ vertically on $C_2$ into $P_2$, project $P_2$ horizontally on $C_3$ into $P_3'$, project $P_3'$ vertically on $C_1$ into $P_1'$, finally project $P_1'$ on $C_2$ into $P'$. If the points $P$ and $P'$ coincide for all points on $C_2$, the three curves are said to have the closure property.

2. *Curves with the Closure Property.* Now consider the one-parameter family of curves given by

$$f(y) + g(a)h(x) + k(a) = 0, \tag{1}$$

defined in the region $x_1 \leqq x \leqq x_2$, $y_1 \leqq y \leqq y_2$, $m \leqq a \leqq n$, where the functions $f$, $g$, $h$, and $k$ are continuous and single-valued, and let a curve $C$ be defined by the equations

$$x = g(a), \qquad y = k(a), \qquad (m \leqq a \leqq n).$$

Then we have the following result.

THEOREM. *Those sets of three curves of* (1), *and only those, which correspond to values of a at which a straight line cuts the curve C, have the closure property.*

PROOF. Consider three curves $C_1$, $C_2$, and $C_3$ corresponding respectively to the parametric values $a_1$, $a_2$, and $a_3$. Now take any point $P(x, y)$ on $C_2$ and project it into $P'(x, y)$ as described above. Making use of (1), we get

$$f(y) - f(y') = -\frac{1}{g(a_3)} \begin{vmatrix} g(a_1) & k(a_1) & 1 \\ g(a_2) & k(a_2) & 1 \\ g(a_3) & k(a_3) & 1 \end{vmatrix}.$$

This determinant will vanish only when the points on the curve $C$ corresponding to the values $a_1$, $a_2$, and $a_3$ lie on a straight line. When the determinant vanishes, we have $f(y)=f(y')$, and hence the points $P$ and $P'$ coincide.

If $C$ is a straight line, the determinant vanishes identically and all curves have the closure property. If $C$ is not cut by any straight line in more than two points, then none of the curves have the closure property.

BUREAU OF ORDNANCE, U. S. NAVY DEPARTMENT

## NOTE ON HOMOGENEOUS FUNCTIONALS*

BY L. S. KENNISON

The classical formula of Euler for functions homogeneous in $n$ variables is as follows.

*Let* $f(x_1, \cdots, x_n)$ *be a differentiable function of the n variables,* $x_1, \cdots, x_n$, *such that*

$$f(\lambda x_1, \cdots, \lambda x_n) = \lambda^p f(x_1, \cdots, x_n). \tag{1}$$

*Then we have*

$$x_1 \frac{\partial f}{\partial x_1} + \cdots + x_n \frac{\partial f}{\partial x_n} = pf(x_1, \cdots, x_n). \tag{2}$$

The following analog of this formula for functionals of one variable was proved by E. Freda.†

*Let* $F\big|\,[f(x)]\,\big|$ *be a functional with a Fréchet differential* $\delta F = \int_0^1 F'\,\big|\,[f(x)]\,;\ \xi\big|\,\delta f(\xi)d\xi + \sum_1^n A_s\big|\,[f(x)]\,\big|\,\delta f(x_s)$, *where* $x_1, \cdots, x_n$ *are points of the interval* (0, 1), *and such that*

$$F\big|\,[\lambda f(x)]\,\big| = \lambda^r F\big|\,[f(x)]\,\big|.$$

*Then*

$$\left\{\frac{\partial}{\partial \lambda} F\big|\,[f(x)(1+\lambda)]\,\big|\right\}_{\lambda=0} = rF\big|\,[f(x)]\,\big|.$$

Theorem 2 of this paper will be a generalization of this theorem of Freda.

The following theorem is classical.

* Presented to the Society, January 19, 1932.

† Rendiconti dei Lincei, (5), vol. 24 (1915), p. 1035.

*Let* $f(x_1, \cdots, x_n)$ *be a differentiable function of the n variables* $x_1, \cdots, x_n$, *such that*

$$f(\lambda x_1, \cdots, \lambda x_n) = K(\lambda) f(x_1, \cdots, x_n) ;$$

*then* $K(\lambda)$ *is a power of* $\lambda$.

In Theorem 1 we generalize this theorem to functionals.

DEFINITION 1. *Let* $Y_1, \cdots, Y_n$ *be n functions each of an arbitrary number (including possibly zero) of variables. If for every determination of the set* $Y_1, \cdots, Y_n$, *(on a certain range), there is determined a function F of a definite number of variables,* $z_1, \cdots, z_m$, *then we say that F is a functional of the n functions* $Y_i$ *and write*

$$F(z_1, \cdots, z_m) = F[Y_1, \cdots, Y_n, z_1, \cdots, z_m].$$

The distinction between $F$ as depending on a $Y$ which is a function of no variables (an independent variable), and on the $z$'s, is largely arbitrary, being a question of what ranges our independent and dependent variables shall have. That is, the dependent variable is not the number $F$, corresponding to the determination of the set $(Y_1, \cdots, Y_n, z_1, \cdots, z_m)$, but the function $F(z_1, \cdots, z_m)$ corresponding to the determination of the set $(Y_1, \cdots, Y_n)$.

Frequently it will be convenient to consider a normed vector space each of whose elements is a suitable determination of a set of functions $(Y_1, \cdots, Y_n)$. We shall denote the norm of this element by $\| Y \|$. If the functional $F(z_1, \cdots, z_m)$ be defined over a portion of such a space, then we may define the Fréchet differential of $F$, when it exists, as follows. (From this point on we shall omit writing the $z$'s.)

DEFINITION 2. *Let* $F[Y_1, \cdots, Y_n]$ *be a functional defined over a portion of a normed vector space of elements* $(Y_1, \cdots, Y_n)$. *Let us consider an element of this space* $(\Delta Y_1, \cdots, \Delta Y_n)$. *Define* $\Delta F[Y_1, \cdots, Y_n; \Delta Y_1, \cdots, \Delta Y_n]$ *to be* $F[Y_1+\Delta Y_1, \cdots, Y_n+\Delta Y_n]-F[Y_1, \cdots, Y_n]$. *Let* $\eta = \|\Delta Y\|$. *Then the Fréchet differential,* $dF[Y_1, \cdots, Y_n; \Delta Y_1, \cdots, \Delta Y_n]$ *is defined to have the following properties:*

(A) *dF is linear and homogeneous* in the* $\Delta Y$'s.

* This means that $dF[Y_1, \cdots, Y_n; \lambda_1 \Delta Y_1 + \mu_1 \Delta' Y_1, \cdots, \lambda_n \Delta Y_n + \mu_n \Delta' Y_n] = A_1\lambda_1 + B_1\mu_1 + \cdots + A_n\lambda_n + B_n\mu_n$, where the $\lambda$'s and $\mu$'s are independent variables. My attention has been called to the fact that this definition differs from Fréchet's in that he uses linear in Property (A) to include distributive and continuous. The continuity is not needed for this paper.

(B) $(\Delta F - dF)/\eta$ *approaches zero with* $\eta$.

The only further property of the Fréchet differential needed below is that

$$\frac{d}{d\lambda} F[\lambda Y_1, \cdots, \lambda Y_n] = dF[\lambda Y ; Y].$$

This follows from an easy generalization of Gateaux's formula* provided $\|\lambda Y\| = |\lambda| \cdot \|Y\|$. Hence we shall not need to specify the particular normed vector space we are using.

THEOREM 1. *Let* $F[Y_1, \cdots, Y_n]$ *denote a functional of the* $n$ *functions* $Y_1, \cdots, Y_n$ *which possesses a Fréchet differential* $dF[Y_1, \cdots, Y_n; \Delta Y_1, \cdots, \Delta Y_n]$, *and such that*

$$F[\lambda Y_1, \cdots, \lambda Y_n] = K(\lambda) F[Y_1, \cdots, Y_n]. \tag{3}$$

*Then* $K(\lambda)$ *is a power of* $\lambda$, *say* $\lambda^p$.

THEOREM 2. *Under the conditions of Theorem* 1,

$$dF[Y_1, \cdots, Y_n ; Y_1, \cdots, Y_n] = pF[Y_1, \cdots, Y_n], \tag{4}$$

*where* $p$ *is the exponent of* $\lambda$ *in the conclusion of that theorem.*

These theorems will be proved together. Differentiating (3) with respect to $\lambda$, we have

$$dF[\lambda Y ; Y] = K'(\lambda) F[Y]. \tag{5}$$

Taking the Fréchet differential of (3), we find

$$\lambda dF[\lambda Y ; \Delta Y] = K(\lambda) dF[Y ; \Delta Y]. \tag{6}$$

Letting $\Delta Y = Y$ in (6), and eliminating $dF[\lambda Y ; Y]$ between (5) and (6), we obtain

$$\frac{\lambda K'(\lambda)}{K(\lambda)} = \frac{dF[Y ; Y]}{F[Y]}. \tag{7}$$

The left side is independent of the $Y$'s and the right of $\lambda$. Hence each is independent of both, say equal to $p$. Integrating the differential equation for $K(\lambda)$ obtained by setting the left side equal to $p$, we have

$$K(\lambda) = C\lambda^p.$$

* Paul Lévy, *Leçons d'Analyse Fonctionnelle*, p. 51.

Letting $\lambda=1$ in (3) we have $C=1$, and Theorem 1 is proved. Letting the right side of (7) equal $p$ gives the conclusion of Theorem 2.

Formula (4) is the analog for functionals of Euler's formula above, and is proved under no restrictions as to the form of the Fréchet differential. We shall now prove the following converse of Theorem 2.

THEOREM 3. *If* $F[Y_1, \cdots, Y_n]$ *denotes a functional of the n functions* $Y_1, \cdots, Y_n$ *which has a Fréchet differential* $dF[Y_1, \cdots, Y_n; \Delta Y_1, \cdots, \Delta Y_n]$, *and if* (4) *holds, then* (3) *also holds, with* $K(\lambda)=\lambda^p$.

Let $F$ be any such functional satisfying (4), and let $R[Y, \lambda] = F[\lambda Y]-\lambda^p F[Y]$. We have

$$R[Y, 1] \equiv 0. \tag{8}$$

Moreover,

$$\frac{dR}{d\lambda} = dF[\lambda Y; Y] - p\lambda^{p-1}F[Y].$$

By (4), we have

$$pF[\lambda Y] = dF[\lambda Y; \lambda Y] = \lambda dF[\lambda Y; Y];$$

hence

$$\frac{dR}{d\lambda} = \frac{p}{\lambda}F[\lambda Y] - p\lambda^{p-1}F[Y] = \frac{p}{\lambda}R[Y; \lambda].$$

Integrating this differential equation, we obtain

$$R[Y; \lambda] = C[Y]\lambda^p. \tag{9}$$

We write our constant of integration as $C[Y]$ as it may be assumed independent of $\lambda$ only. Letting $\lambda=1$, and using (8) we have $C[Y]=0$. Hence $R[Y; \lambda]=F[\lambda Y]-\lambda^p F[Y]=0$.

BROOKLYN COLLEGE OF THE CITY OF NEW YORK

# NOTE ON THE ORTHOGONALITY OF TCHEBYCHEFF POLYNOMIALS ON CONFOCAL ELLIPSES*

BY J. L. WALSH

In the study of polynomial expansions of analytic functions in the complex plane, two different definitions of orthogonality are current:

$$(1) \quad \int_C n(z)p_j(z)p_k(z)\,dz = 0, \text{ or } \int_C p_j(z)q_k(z)dz = 0, \ (j \neq k),$$

$$(2) \quad \int_C n(z)p_j(z)\overline{p_k(z)}\,|\,dz\,| = 0, \qquad (j \neq k).$$

Definition (1) in one form or the other (the second form of (1) may be called biorthogonality) is of frequent use, for instance in connection with the Legendre polynomials,† and has the great advantage that if the functions involved are analytic, the contour of integration $C$ may be deformed without altering the orthogonality property. Definition (2) is of importance—indeed inevitable—when one wishes to study approximation on $C$ in the sense of least squares, and it is entirely with definition (2) that we shall be concerned in the present note. More explicitly, condition (2) may be described as orthogonality with respect to the norm function $n(z)$, ordinarily chosen as continuous and positive or at least non-negative on $C$.

An illustration of (1), where $C$ is the unit circle $|z| = 1$, is the set of functions $1, z, z^2, \cdots, n(z) \equiv 1$. An illustration of (2), where $C$ is the unit circle, is the set of functions $\cdots, z^{-2}, z^{-1}, 1, z, z^2, \cdots, n(z) \equiv 1$:

$$\int_C z^j\bar{z}^k\,|\,dz\,| = \int_C \frac{z^j}{z^k}\,\frac{dz}{iz} = 0, \qquad (j \neq k).$$

The connection of orthogonality in the sense of (2) with ap-

* Presented to the Society, October 28, 1933.

† The reader may refer to Heine, *Kugelfunktionen*, 1878; Darboux, Journal de Mathématiques, (3), vol. 4 (1878), pp. 5–56, and pp. 377–416; Geronimus, Transactions of this Society, vol. 33 (1931), pp. 322–328.

proximation in the sense of least squares has long been known.* The application to polynomial expansions on curves in the complex plane is due to Szegö† in the case $n(z)\equiv 1$ and to Walsh‡ in the more general case. The most important theorem which concerns us here is the following, which is due to Szegö ($n(z)\equiv 1$, $C$ analytic), Smirnoff ($n(z)\equiv 1$, $C$ rectifiable and subject to auxiliary condition), and Walsh, loc. cit., ($n(z)$ positive and continuous, $C$ rectifiable).

*Let $C$ be a rectifiable Jordan curve and let the function $w=\phi(z)$ map the exterior of $C$ onto the exterior of $|w|=1$ so that the points at infinity correspond to each other. Let the curve $|\phi(z)|=R>1$ be generically denoted by $C_R$.*

*If the function $f(z)$ is analytic interior to $C_\rho$ but has a singularity on $C_\rho$, and if*

$$f(z)\sim \sum a_k p_k(z),$$

$$a_k\int_C n(z)p_k(z)\overline{p_k(z)}\,|\,dz\,| = \int_C n(z)f(z)\overline{p_k(z)}\,|\,dz\,|, \tag{3}$$

*is the formal expansion of $f(z)$ in terms of the polynomials $p_k(z)$ of respective degrees $k$ orthogonal on $C$ with respect to the function $n(z)$ positive and continuous on $C$, then series (3) converges to $f(z)$ interior to $C_\rho$, uniformly on any closed point set interior to $C_\rho$, and converges uniformly in no region containing in its interior a point of $C_\rho$.*

There is no series other than (3) of the form $\sum b_k p_k(z)$ which converges to $f(z)$ uniformly on $C$.

This theorem is valid also in the limiting case that $C$ is a line segment or other rectifiable Jordan arc. The case that $C$ is a line segment has long been studied and by numerous writers; for instance the weight function $n(z)\equiv 1$ leads to expansions in Legendre polynomials treated for complex values of the argument by C. Neumann in 1862. When $C$ is a line segment, the curves $C_R$ are ellipses whose foci are the ends of the segment.

The theorem naturally raises the question as to whether (3) can be both the formal expansion of $f(z)$ on $C$ and the formal expansion of $f(z)$ on some $C_{\rho'}$, $\rho'<\rho$, or in other words whether

* See for instance Kowalewski, *Determinantentheorie*, 1909, p. 335.

† Mathematische Zeitschrift, vol. 9 (1921), pp. 218–270.

‡ Transactions of this Society, vol. 32 (1930), pp. 794–816.

the same set of polynomials $p_k(z)$ can result from orthogonalization (in the sense corresponding to (2)) of the set $1, z, z^2, \cdots$, on two different curves. An obvious illustration is the case that $C$ is the unit circle. The polynomials $1, z, z^2, \cdots$ are orthogonal with weight function unity on *every* circle whose center is the origin, and the formal expansion (3) of a function $f(z)$ analytic at the origin is the same on every such circle containing on or within it no singularity of $f(z)$.

It is the object of the present note to show that *the Tchebycheff polynomials found by orthogonalization of* $1, z, z^2, \cdots$ *on the line segment* $C: -1 \leqq z \leqq +1$ *with respect to the norm function* $(1-z^2)^{-1/2}$ *are also orthogonal with respect to suitable norm functions on all the corresponding curves* $C_R$, *which are ellipses with the common foci* $(-1, +1)$.

We shall find it more convenient to transform our problem to the $w$-plane. The exterior of $C: -1 \leqq z \leqq +1$ is transformed onto the exterior of $\gamma: |w| = 1$ by the transformation

$$z = \frac{1}{2}\left(w + \frac{1}{w}\right), \tag{4}$$

so that the points at infinity correspond to each other. Let the polynomials $p_0(z) \equiv 1$, $p_1(z)$, $p_2(z), \cdots$ result from orthogonalizing on $\gamma$ the linearly independent set $1, z, z^2, \cdots$ with norm function unity. We shall prove that the polynomials $p_k(z)$ form an orthogonal set on $\Gamma: |w| = R > 1$ with norm function unity. For the sake of reference we write the equations

$$\begin{aligned} z &= \frac{1}{2}\left(w + \frac{1}{w}\right), \quad z^2 = \frac{1}{4}\left(w^2 + 2 + \frac{1}{w^2}\right), \\ z^3 &= \frac{1}{8}\left(w^3 + 3w + \frac{3}{w} + \frac{1}{w^3}\right), \cdots, \end{aligned} \tag{5}$$

whence, on $\Gamma$,

$$\begin{aligned} \bar{z} &= \frac{1}{2}\left(\frac{R^2}{w} + \frac{w}{R^2}\right), \ \bar{z}^2 = \frac{1}{4}\left(\frac{R^4}{w^2} + 2 + \frac{w^2}{R^4}\right), \\ \bar{z}^3 &= \frac{1}{8}\left(\frac{R^6}{w^3} + \frac{3R^2}{w} + \frac{3w}{R^2} + \frac{w^3}{R^6}\right), \cdots. \end{aligned} \tag{6}$$

We need merely prove that the polynomial $p_n(z)$ is orthogonal to each of the polynomials $p_0(z)$, $p_1(z)$, $\cdots$, $p_{n-1}(z)$, and it is sufficient to show that $p_n(z)$ is orthogonal to each of the functions $1, z, \cdots, z^{n-1}$. We shall prove this by induction.

We have by hypothesis

$$\int_\gamma p_n(z)\,|\,dw\,| = 0, \tag{7}$$

and we show first that we have also

$$\int_\Gamma p_n(z)\,|\,dw\,| = 0. \tag{8}$$

Direct computation gives us $|\,dw\,| = R\,dw/(iw)$ for $w$ on $\Gamma$. When this substitution is made in (7) and (8), it is seen that the integral in (8) is except for the factor $R$ precisely the integral in (7); the function $p_n(z)$ has no singularities in the $w$-plane except at the origin and at infinity. Hence equation (8) follows at once.

Let us now suppose

$$\int_\Gamma p_n(z)\,|\,dw\,| = 0, \quad \int_\Gamma p_n(z)\bar{z}\,|\,dw\,| = 0, \cdots, \tag{9}$$

$$\int_\Gamma p_n(z)\bar{z}^{k-1}\,|\,dw\,| = 0, \quad (k-1 < n-1).$$

We are to prove that

$$\int_\Gamma p_n(z)\bar{z}^k\,|\,dw\,| = 0. \tag{10}$$

From inspection of equations (6) and by virtue of equations (9), it follows that the integral in (10) can be written

$$\frac{1}{2^k}\int_\Gamma p_n(z)\left(\frac{R^{2k}}{w^k}+\frac{w^k}{R^{2k}}\right)\frac{R\,dw}{iw}. \tag{11}$$

If we consider the various terms in $p_n(z)$ as expressed by means of (5), and omit such of those terms as obviously make no contribution to the integral (11), we see that (11) can be written

$$A_{nk}\int_\Gamma \left(w^k+\frac{1}{w^k}\right)\left(\frac{R^{2k}}{w^k}+\frac{w^k}{R^{2k}}\right)\frac{R\,dw}{iw} \tag{12}$$

$$= 2\pi A_{nk}R\left[R^{2k}+\frac{1}{R^{2k}}\right],$$

where $A_{nk}$ is a suitable constant independent of $R$, easy to compute in terms of the coefficients of the powers of $z$ in $p_n(z)$. By hypothesis the polynomials $p_n(z)$ are orthogonal on the circle $\gamma$. Hence the integrals corresponding to (10), (11), and (12) vanish for $R=1$. Thus we have $A_{nk}=0$, so (10) is established and the orthogonality on $\Gamma$ of the set $p_k(z)$ with respect to the norm function unity is completely proved.

It remains to study the norm function in the $z$-plane, and to identify our present polynomials with the polynomials of Tchebycheff. From (4) we have for $|w|=R$,

$$dz=\frac{1}{2}\left(1-\frac{1}{w^2}\right)dw, \qquad \left|\frac{dw}{dz}\right|=\frac{2R}{\left|w-\frac{1}{w}\right|}=\frac{R}{|(1-z^2)^{1/2}|}.$$

The circle $|w|=1$ corresponds to the segment $-1\leqq z\leqq +1$ (counted twice, or in the study of orthogonality, only once if we prefer, for the norm function is single-valued on the segment). We clearly have

$$\int_{-1}^{1} n(z)p_n(z)\overline{p_k(z)}\,|\,dz\,|=\int_{\gamma} n(z)p_n(z)\overline{p_k(z)}\,|\,dw\,|\,\left|\frac{dz}{dw}\right|,$$

so the corresponding norm function on the segment $-1\leqq z\leqq +1$ is $1/|(1-z^2)^{1/2}|$. The norm function on an arbitrary ellipse whose foci are $+1$ and $-1$ is $R/|(1-z^2)^{1/2}|$, where the ellipse is represented by $|z-1|+|z+1|=R+1/R$, $R>1$. The norm function on any curve can be modified by any non-vanishing constant factor, so if we prefer we can still express the norm function on any ellipse $C_R$ as $|1-z^2|^{-1/2}$.

In the present note we have studied orthogonality on a particular set of confocal ellipses; a simple transformation yields the analogous results for orthogonality of corresponding polynomials on any set of confocal ellipses.

The writer is not aware of any case other than the present one, where orthogonalization in the sense of (2) of the set $1, z, z^2, \cdots$, on a curve $C_1$ with respect to a norm function $n_1(z)$, is equivalent to orthogonalization of that set on another curve $C_2$ with respect to a norm function $n_2(z)$, except where $C_1$ and $C_2$ are concentric circles.

HARVARD UNIVERSITY

# DERIVATIVES, DIFFERENCE QUOTIENTS, AND TAYLOR'S FORMULA*

BY HASSLER WHITNEY†

1. *Introduction.* Let $f(x)$ be defined in the closed interval $I$. If $f(x)$ has a continuous $m$th derivative, it can be expanded in a Taylor's formula with $m+1$ terms plus remainder; the $m$th difference quotient of $f(x)$ approaches $d^m f(x)/dx^m$ uniformly. If $f(x)$ is a polynomial of degree at most $m-1$, then the $m$th difference quotient is identically zero. The object of the present note is to prove converses of these theorems. The results hold also in an open interval, as they hold in every closed subinterval.

2. *Difference Quotients.* Given a function $f(x)$ defined in $I$, the $p$th difference quotient is defined by the equations $\Delta_h^0 f(x) = f(x)$, and

$$\Delta_h^p f(x) = \frac{1}{h^p} \sum_{i=0}^{p} (-1)^{p-i} \binom{p}{i} f(x + ih) \tag{1}$$

$$= \frac{1}{h} [\Delta_h^{p-1} f(x + h) - \Delta_h^{p-1} f(x)]$$

for $p > 0$. We say $\Delta_h^p f(x) \to f_p(x)$ uniformly in $I$ if for every $\epsilon > 0$ there is a $\delta > 0$ such that $|\Delta_h^p f(x) - f_p(x)| < \epsilon$ for every $x$ in $I$ and every $h$, $|h| < \delta$.‡

(a) Suppose $f_0(x), f_1(x), \cdots, f_m(x)$ are defined in $I$, and

$$(2)\quad f_0(x + h) = f_0(x) + \frac{1}{1!} f_1(x)h + \cdots + \frac{1}{m!} f_m(x)h^m + R(x, h),$$

where $R(x, h)/h^m \to 0$ uniformly in $I$ as $h \to 0$. If we form the $p$th difference quotient, we find§

---

* Presented to the Society, June 23, 1933.

† National Research Fellow.

‡ We always suppose that the values of $x$ under consideration (here, $x+ih$ for $i=0, \cdots, p$) lie in $I$.

§ If we solve the linear equations (setting $0^0 = 1$)

$$0^j u_0 + 1^j u_1 + \cdots + p^j u_p = p!\delta_{jp}, \qquad (j = 0, \cdots, p),$$

we find $u_i = (-1)^{p-i}\binom{p}{i}$; hence $\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i} i^j = 0$, $(j < p)$, and $= p!$, $(j = p)$.

$$(3)\quad \Delta_h^p f_0(x) = \frac{1}{h^p}\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}\left[\sum_{j=0}^{m}\frac{f_j(x)}{j!}(ih)^j + R(x,ih)\right]$$

$$= \sum_{j=0}^{m}\frac{f_j(x)}{j!}h^{j-p}\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^j + \frac{1}{h^p}R_p(x,h)$$

$$= f_p(x) + \sum_{j=p+1}^{m}\frac{f_j(x)}{j!}h^{j-p}\sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}i^j + \frac{1}{h^p}R_p(x,h),$$

where

$$(4)\qquad R_p(x,h) = \sum_{i=0}^{p}(-1)^{p-i}\binom{p}{i}R(x,ih).$$

From (2) we see that $f_0(x)$ is continuous; hence $\Delta_h^p f_0(x)$ is continuous ($h$ fixed, $p=1,\cdots,m$). Setting $p=m$ in (3), we see that $\Delta_h^m f_0(x)\to f_m(x)$ uniformly; hence $f_m(x)$ is continuous. Having proved that $\Delta_h^q f_0(x)\to f_q(x)$ uniformly and $f_q(x)$ is continuous, $(q=m, m-1,\cdots,p+1)$, (3) shows that $\Delta_h^p f_0(x)\to f_p(x)$ uniformly, and hence $f_p(x)$ is continuous, $(p=1,\cdots,m)$.

(b) Suppose $f(x)=f_0(x)$ and $d^pf(x)/dx^p$ exists and equals the continuous function $f_p(x)$, $(p=1,\cdots,m)$. Then (2) holds, by Taylor's theorem, and hence $\Delta_h^p f(x)\to d^pf(x)/dx^p$ uniformly, $(p=1,\cdots,m)$.

(c) Suppose $f(x)=a_0+a_1x+\cdots+a_mx^m$ is a polynomial of degree at most $m$. Then a Taylor's formula (2) holds with $f_m(x)\equiv m!a_m$ and $R(x,h)\equiv 0$, and using (3) with $p=m$, we have $\Delta_h^m f(x)\equiv m!a_m$. If $f(x)$ is of degree at most $m-1$, $\Delta_h^m f(x)\equiv 0$.

3. *Rolle's Theorem for Difference Quotients.* We shall prove first the following lemma.

LEMMA 1. *If $k_0<k_1<\cdots<k_m$ are integers, $h$ is $>0$, and*

$$(5)\qquad (-1)^{m-i}f(x+k_ih)\geqq 0,\quad (i=0,\cdots,m),$$

*then there is an integer $k_0^{(m)}$ $(k_0\leqq k_0^{(m)}<k_m)$ such that*

$$(6)\qquad \Delta_h^m f(x+k_0^{(m)}h)\geqq 0.$$

As $f(x+k_mh)\geqq 0$ and $f(x+k_{m-1}h)\leqq 0$, there is a $k_{m-1}^{(1)}$,

$(k_{m-1} \leqq k_{m-1}^{(1)} < k_m)$, such that $\Delta_h^1 f(x+k_{m-1}^{(1)}h) \geqq 0$. In this manner we find numbers $k_0^{(1)}, \cdots, k_{m-1}^{(1)}$, $(k_{i-1} \leqq k_{i-1}^{(1)} < k_i)$, such that

$$(-1)^{m-1-i}\Delta_h^1 f(x + k_i^{(1)}h) \geqq 0, \quad (i = 0, \cdots, m-1).$$

By the same method, using $\Delta_h^1 f(x)$ in place of $f(x)$, we find numbers $k_0^{(2)}, \cdots, k_{m-2}^{(2)}, (k_{i-1}^{(1)} \leqq k_{i-1}^{(2)} < k_i^{(1)})$, such that

$$(-1)^{m-2-i}\Delta_h^2 f(x + k_i^{(2)}h) \geqq 0, \quad (i = 0, \cdots, m-2).$$

Continuing in this manner we find, finally, the required number $k_0^{(m)}$.

4. THEOREM 1. *Let $f(x)$ be measurable in the closed interval $I$. A necessary and sufficient condition that $f(x)$ be a polynomial of degree at most $m-1$ is that $\Delta_h^m f(x) \to 0$ uniformly.**

The theorem is not true without the measurability condition. For the discontinuous functions defined by G. Hamel† are seen to have the property $\Delta_h^r f(x) \equiv 0$.

The necessity of the condition follows from §2 (c); we must prove the sufficiency. We shall prove first the following lemma.

LEMMA 2. *Let $f(x)$ satisfy the conditions of the theorem. Let $r_1, r_2, \cdots, r_m$ be rational numbers. Take a fixed number $a$ and a fixed $t$. Let $P(x)$ be the polynomial of degree at most $m-1$ such that $f(a+r_it) = P(a+r_it)$, $(i=1, \cdots, m)$. Then if $r$ is any rational number, $f(a+rt) = P(a+rt)$.*

Suppose that the lemma is not true. Then for some rational $r_0$, $f(a+r_0t) \neq P(a+r_0t)$. Let

$$Q(x) = c_0 + c_1x + \cdots + c_mx^m, \qquad (c_m \neq 0),$$

be the polynomial of degree $m$ such that $Q(a+r_it) = f(a+r_it)$, $(i=0, \cdots, m)$. Set $\phi(x) = f(x) - Q(x)$; then $\phi(a+r_it) = 0$, $(i=0, \cdots, m)$, and by §2 (c),

$$\Delta_h^m \phi(x) = \Delta_h^m f(x) - m!c_m \to -m!c_m$$

uniformly as $h \to 0$. Hence we can take a $\delta > 0$ so that $\Delta_h^m \phi(x) < 0$ or $> 0$ for all $x$ in $I$ and $h < \delta$ according as $c_m > 0$ or $c_m < 0$. As

* The case that $f(x)$ is continuous and $\Delta_h^m f(x) \equiv 0$ has been considered by Anghelutza, Mathematica (Cluj), vol. 6 (1932), pp. 1–7.

† Mathematische Annalen, vol. 60(1905), p. 461, equation (2).

the $r_i$ are rational, there is a number $r$ such that $rt<\delta$ and the numbers $a+krt$ ($k$ an integer) include the numbers $a+r_it$. By Lemma 1, there are integers $k'$ and $k''$ such that $\Delta_{rt}^m\phi(a+k'rt)\geqq 0$ and $\Delta_{rt}^m\phi(a+k''rt)\leqq 0$, a contradiction, proving the lemma.

5. *Proof of Theorem* 1. If we define $P(x)$ as in the lemma, $a$ and $t$ being rational, then $f(x)=P(x)$ at all rational points of $I$. If $f(x)$ is continuous, it follows that $f(x)\equiv P(x)$ in $I$. To complete the proof of the theorem, we must show that if $f(x)\not\equiv P(x)$, then $f(x)$ is not measurable.

Suppose there is a number $a$ in $I$ such that $f(a)\neq P(a)$. If $Q(x)$ is the polynomial of degree at most $m-1$ such that $f(x)=Q(x)$ at points $a, a+r_2, \cdots, a+r_m$, ($r_2, \cdots, r_m$ rational), then $f(x)=Q(x)$ at all points $a+r$, ($r$ rational), by the lemma. Set $\sigma=|Q(a)-P(a)|$, and take $\delta>0$ so that

$$(7)\qquad |P(x)-P(a)|<\frac{\sigma}{4},\qquad |Q(x)-Q(a)|<\frac{\sigma}{4},\qquad (|x-a|\leqq\delta).$$

Take $\eta>0$ so that if $R(x)$ is any polynomial of degree at most $m-1$ such that $|R(i)|\leqq\eta$, ($i=1, \cdots, m$), then $|R(0)|<\sigma/4$.* By a change of variable, we see then that for any $x$, $h$, and $y_0$, *if* $|R(x+ih)-y_0|\leqq\eta$, ($i=1, \cdots, m$), *then*

$$|R(x)-y_0|<\sigma/4.$$

If $f(x)$ is measurable, there is a number $y_0$ such that the set of points $E$ in $(a-\delta, a+\delta)$ (and in $I$) for which $|f(x)-y_0|\leqq\eta$ is of positive measure. Let $I'$ be a closed subinterval of $(a-\delta, a+\delta)$ such that if $E_m=E\cdot I'$, then†

$$(8)\qquad \text{meas } (E_m)>\frac{m^2}{m^2+1}\text{ meas } (I').$$

Either $|y_0-P(a)|\geqq\sigma/2$ or $|y_0-Q(a)|\geqq\sigma/2$, say the latter. Let $b$ be a number in $I'$ such that $f(b)=Q(b)$, (take $b-a$ rational); then, using (7), $|f(b)-y_0|>\sigma/4$.

Let $S$ be the set of numbers $s$ such that $b+ms$ is in $E_m$, and $E_i$ the set of numbers $b+is$, where $s$ is in $S$, ($i=1, \cdots, m-1$).

* That this can be done follows easily from the fact that $\Delta_1^m R(0)=0$; see §2 (c).

† See Hobson, *Functions of a Real Variable*, vol. 1, 3d ed., 1923, p. 194.

Set $E_i' = E_i \cdot E_m$, and let $S_i$ be the set of numbers $s$ in $S$ such that $b+is$ is in $E_i'$, $(i=1, \cdots, m)$. There is no number $s_0$ in every $S_i$. For if there were, we would have simultaneously

$$(9)\quad |f(b+is_0) - y_0| \leqq \eta,\ (i=1, \cdots, m),\ |f(b) - y_0| > \sigma/4.$$

Hence by our choice of $\eta$, if $R(x)$ is the polynomial of degree at most $m-1$ such that $R(b+is_0) = f(b+is_0)$, $(i=1, \cdots, m)$, then $R(b) \neq f(b)$. But this contradicts Lemma 2.

Consequently, every number $s$ of $S$ is in some set $S-S_i$, and hence for some $j$, meas $(S-S_j) \geqq$ meas $(S)/m$. Therefore

$$\text{meas } (E_j - E_j') \geqq \frac{\text{meas } (E_j)}{m} \geqq \frac{\text{meas } (E_m)}{m^2}.$$

As $E_m$ and $E_j - E_j'$ have no common points, this with (8) gives

$$(10)\quad \text{meas } [E_m + (E_j - E_j')] \geqq \text{meas } (E_m)\left[1 + \frac{1}{m^2}\right] > \text{meas } (I').$$

But this contradicts the fact that $E_m + E_j$ lies in $I'$. Hence $f(x)$ is not measurable, and the theorem is proved.

THEOREM 2. *Let $f(x)$ be measurable in the closed interval $I=(\alpha, \beta)$. A necessary and sufficient condition* that $d^m f(x)/dx^m$ exist and equal $f_m(x)$ is that $\Delta_h^m f(x) \to f_m(x)$ uniformly in $I$.*

---

* A direct proof of this theorem may be given as follows, as suggested by Birkhoff. The function $f(kh)$, $(h=1/p,\ k$ and $p$ integral), may be expressed in terms of $\Delta_h^m f(x)$ by the formula

$$(12)\quad f(kh) = \sum_{i=0}^{m-1} a_i (kh)^i + \frac{h^m}{(m-1)!} \sum_{l=0}^{k-1} (k-l-1)(k-l-2) \cdots (k-l-m+1) \Delta_h^m f(lh),$$

where the $a_i$ are determined so that $f(sph) = f(s)$, $(s=0, \cdots, m-1)$. We solve a set of linear equations with a Vandermonde determinant, and find

$$(13)\quad a_i = \sum_{s=0}^{m-1} \eta_{is} \left[ f(s) - \frac{h^m}{(m-1)!} \sum_{l=0}^{sp-1} (sp-l-1) \cdots (sp-l-m+1) \Delta_h^m f(lh) \right],$$

The necessity of the condition was proved in §2 (b). To prove the sufficiency, we show first that $f_m(x)$ is continuous. Take $\delta$ so small that $|\Delta_h^m f(x) - f_m(x)| < \epsilon/2$ for $|h| < \delta$. Take any two points $x_1$ and $x_2$ of $I$ such that $x_2 - x_1 = mh$, $|h| < \delta$. Then $|\Delta_h^m f(x_1) - f_m(x_1)| < \epsilon/2$, $|\Delta_{-h}^m f(x_2) - f_m(x_2)| < \epsilon/2$. But $\Delta_{-h}^m f(x_2) = \Delta_h^m f(x_1)$; hence $|f_m(x_2) - f_m(x_1)| < \epsilon$.

Define the $m$-fold integral

$$(11) \quad g(x) = \int_a^x \cdots \int_a^{x_2} \int_a^{x_2} f_m(x_1)dx_1dx_2 \cdots dx_m;$$

then $d^m g(x)/dx^m = f_m(x)$ in $I$, and by §2 (b), $\Delta_h^m g(x) \to f_m(x)$ uniformly in $I$. Set $\phi(x) = f(x) - g(x)$. Then $\Delta_h^m \phi(x) \to 0$ uniformly; hence $\phi(x)$ is a polynomial of degree at most $m-1$ (Theorem 1), and therefore $f(x)$ has a continuous $m$th derivative in $I$, and

$$\frac{d^m}{dx^m} f(x) = \frac{d^m}{dx^m} \phi(x) + \frac{d^m}{dx^m} g(x) = f_m(x).$$

THEOREM 3. *A necessary and sufficient condition that the function $f(x) = f_0(x)$ defined in $I$ have a continuous $m$th derivative is that there exist functions $f_1(x), \cdots, f_m(x)$ such that (2) holds. In this case, $d^p f(x)/dx^p = f_p(x)$, $(p = 1, \cdots, m)$.*

The necessity of the condition is a consequence of Taylor's formula. To prove the sufficiency, §2 (a) shows that $\Delta_h^p f(x) \to f_p(x)$ uniformly as $h \to 0$; consequently†, by Theorem 2, $d^p f(x)/dx^p$ exists and equals $f_p(x)$, $(p = 1, \cdots, m)$.

HARVARD UNIVERSITY

---

where the $\eta_{is}$ are numerical coefficients. If in the above equations we replace $p$ by $p_j = 2^j p$, $h$ by $h_j = h/2^j$, and $k$ by $k_j = 2^j k$, and set $r = k_j h_j = kh$, then as $\Delta_{k_j}^m f(x) \to f_m(x)$ uniformly, passing to the limit $j = \infty$ gives

$$(14) \quad (r) = \sum_{i=0}^{m-1} r^i \sum_{s=0}^{m-1} \eta_{is} \left[ f(s) - \frac{1}{(m-1)!} \int_0^s (s-t)^{m-1} f_m(t)dt \right] + \frac{1}{(m-1)!} \int_0^r (r-t)^{m-1} f_m(t)dt,$$

for any rational $r > 0$. If $f(x)$ is continuous, this is true for all $r > 0$ and, the theorem follows immediately on differentiating. (The restriction $r > 0$ may of course be replaced by the restriction $r > -c$ for any $c$.)

† A direct proof of this theorem is given by the author in a paper entitled *Differentiable functions defined in closed sets I*, Theorem IV.

# LINEAR ASSOCIATIVE ALGEBRAS OF INFINITE ORDER WHOSE ELEMENTS SATISFY FINITE ALGEBRAIC EQUATIONS*

BY H. H. CONWELL

1. *Introduction.* It is the purpose of this paper to investigate linear associative algebras of infinite order, whose elements satisfy finite algebraic equations with coefficients in a field $\Xi$. The definition† of an algebra, and the first three postulates‡ assumed, will be the same as those employed by L. E. Dickson for a finite algebra, but in place of Dickson's postulates for a finite basis we shall employ postulates IV and V as follows.

POSTULATE IV. *There exists in $A$ a set of elements§ $U$ of such a nature that for every $a \neq 0$ there is determined uniquely a positive integer $n$, a set of distinct elements $u_1, u_2, \cdots, u_n$ of $U$, and $n$ non-zero elements $\xi_1, \xi_2, \cdots, \xi_n$ of $\Xi$ such that $a = \sum_{i=1}^{n} \xi_i u_i$.*

POSTULATE V. *For every element $a$ of $A$ there exists a polynomial function $h(\lambda)$, with coefficients in $\Xi$, such that $h(a) = 0$.*

2. *Idempotent Elements; Semi-Nilpotent Algebras.*

THEOREM 1. *Every algebra $A$ contains an idempotent element unless all its elements are nilpotent.*

For if $a$ is any non-zero non-nilpotent element of $A$ whose minimum‖ equation is $g(\lambda) = 0$, of degree $n$, then the finite subalgebra $B = (a, a^2, a^3, \cdots, a^n)$ of $A$, contains an idempotent element.

THEOREM 2. *If an algebra $A$ is not semi-nilpotent,¶ but con-*

* Presented to the Society, April 9, 1932.

† L. E. Dickson, *Algebras and their Arithmetics*, University of Chicago Press, pp. 9–11, cited hereafter as Dickson.

‡ For the convenience of the reader, references will be made to Dickson, wherever possible, whether or not this constitutes the original source.

§ The set $U$ is not assumed enumerable except in the example of §2, the subalgebra $M$ of $A$ in Theorem 11, and in Theorem 13.

‖ The equation $g(\lambda) = 0$ of lowest degree, with rational coefficients and leading coefficient unity, for which $g(a) = 0$, will be called the minimum equation of $a$.

¶ An algebra $A$ will be called semi-nilpotent if all its elements are nilpotent, and semi-simple if it contains no properly nilpotent elements.

*tains a maximal* semi-nilpotent invariant sub-algebra $K$, then $K$ is unique.*

For if $K'$ is any other semi-nilpotent invariant sub-algebra of $A$, then $K+K'$ is invariant in $A$. Moreover, if $k_1$ and $k_1'$ are any two elements of $K$ and $K'$, respectively, then $(k_1+k_1')^{\alpha\beta} = (k_\alpha+k_1'^{\alpha})^{\beta} = k_\alpha{}^{\beta} = 0$, where $k_\alpha$ is in $K$ and the indices† of $k_1'$ and $k_\alpha$ are $\alpha$ and $\beta$, respectively. Therefore $K+K'$ is a semi-nilpotent invariant sub-algebra of $A$. But $K$ is maximal, hence $K+K'=K$, or $K'$ is contained in $K$.

LEMMA. *Any non-zero element $a$ of an algebra $A$, which is not properly nilpotent in $A$, possesses an inverse with respect to some idempotent element $e$ of $A$, that is, an element $x$ such that $ax=e$.*

For otherwise, the sub-algebra $aA$ contains no idempotent element and hence is semi-nilpotent and $a$ is properly nilpotent in $A$, contrary to hypothesis.

THEOREM 3. *If $a$ and $b$ are any two properly nilpotent elements of an algebra $A$, then their sum $a+b$ is also properly nilpotent in $A$.*

The contrary assumption necessitates the existence in $A$ of elements $x$ and $e$ such that $(a+b)x=ax+bx=p+q=e$, where $e$ is idempotent and $epe$ and $eqe$ are zero or properly nilpotent. Therefore, if $\alpha$ is the index of $epe$, $(epe)^{\alpha}=(e-eqe)^{\alpha}=0$, and hence $e=a_1qe$, ($a_1$ in $A$). But $a_1qe$ is properly nilpotent in $A$, whereas $e$ is idempotent. This contradiction implies that $a+b$ is properly nilpotent in $A$.

THEOREM 4. *An algebra $A$ which is not semi-nilpotent contains properly nilpotent elements if and only if it possesses a maximal semi-nilpotent invariant sub-algebra $K$, and then the properly nilpotent elements of $A$ coincide with the non-zero elements of $K$.*

The first part of the theorem follows at once from the definition of $K$. To prove the second part, represent the aggregate of properly nilpotent elements in $A$ by $B$. By means of Theorem 3 we can show that $B$ is a semi-nilpotent invariant sub-algebra of $A$, and since it contains all the properly nilpotent elements of $A$ it is maximal and hence is identical with $K$ (Theorem 2).

* Dickson, p. 32.

† If $\alpha$ is an integer such that $a^{\alpha}=0$, but $a^{\alpha-1}\neq 0$, $\alpha$ is the index of $a$.

An algebra $A$ may be decomposed into the form

$$A = I + eR + Le + eAe, \tag{1}$$

in which $e$ is idempotent, $I$ contains all elements $x$ of $A$ such that $ex = xe = 0$, $R = I + eR$ contains all elements $y$ of $A$ such that $ye = 0$, and $L = I + Le$ contains all elements $z$ of $A$ such that $ez = 0$.

THEOREM 5. *If $e$ is a principal idempotent element of $A$, every non-zero element of $I$, $L$, and $R$ in* (1) *is properly nilpotent.*

PROOF. $(Le)^2 = 0 = (eR)^2$. Since $eLR = LRe = 0$, it follows that $LR \leqq I$. If $x$ and $z$ are any two non-zero elements of $I$ and $Le$, respectively, then $(x+z)^n = x^n + z_{n-1}$, ($z_{n-1}$ in $Le$). Since $x$ is nilpotent with an index $\alpha$, $(x+z)^{2\alpha} = z_{\alpha-1}^2 = 0$, ($z_{\alpha-1}$ in $Le$). Thus each element of $L$ is zero or nilpotent. Likewise each element of $R$ is zero or nilpotent.

$ARe = 0 = Re$, and $eLA = 0 = eL$, hence $AR \leqq R$ and $LA \leqq L$. Therefore the elements of $R$ and $L$, and hence of their intersection $I$, are properly nilpotent in $A$.

THEOREM 6. *Every algebra $A$ with a principal idempotent element, but no principal unit, has a semi-nilpotent invariant sub-algebra $K$.*

This theorem is a direct consequence of Theorems 4 and 5.

*Any semi-simple algebra $A$ of finite order which is not simple is reducible.** The proof of this theorem depends upon the theorem, *Any invariant sub-algebra of a semi-simple algebra of finite order possesses a principal unit.* The following example exhibits the failure of the latter theorem for infinite algebras, and the sub-algebra $B$ illustrates the failure of two other theorems.

(1) *Every finite linear associative algebra which is not nilpotent contains a principal idempotent element.**

(2) *Every finite algebra with no principal unit has a nilpotent invariant sub-algebra.**

EXAMPLE. Let $A = (e, u_1, u_2, u_3, \cdots)$ in which $eu_i = u_i e = u_i$, $e^2 = e$, $u_i^2 = u_i$, $u_i u_j = u_j u_i = 0$, $i \neq j$. Then $A$ is a semi-simple algebra with the principal unit $e$, and an invariant sub-algebra

* Dickson, pp. 49–53.

$B=(u_1, u_2, u_3, \cdots)$ which contains no principal unit, no principal idempotent element and no nilpotent invariant sub-algebra.

3. *Difference Algebras.** THEOREM 7. *If an algebra $A$ is not semi-nilpotent, but contains the maximal semi-nilpotent invariant sub-algebra $K$, then the difference algebra $A-K$ contains no semi-nilpotent invariant sub-algebra.*

For suppose $A-K$ has a semi-nilpotent invariant sub-algebra $K_1$. The elements of $A-K$ are classes $[a]$ of elements of $A$. Represent by $B$ all elements of $A$ belonging to classes $[b]$ of $A-K$ which are in $K_1$. From the definition of $K_1$, $B$ is an algebra. If $a$ and $b$ are any two elements of $A$ and $B$, respectively, then $[a][b]=[ab]$ is in $K_1$ and also in $B-K$. Hence $B$ is invariant in $A$, and $B-K=K_1$, or $B>K$. All elements of $B$ are nilpotent and hence $B$ is a semi-nilpotent invariant sub-algebra of $A$. But $B>K$ contrary to the hypothesis on $K$, therefore $A-K$ contains no semi-nilpotent invariant sub-algebra.

THEOREM 8. *Every idempotent class $[u]$ of $A-K$ contains idempotent elements of $A$.*

PROOF. $[u]=[u^2]=[u^3]=\cdots=[u^\alpha]$, and $[u]\neq[0]$. Hence $u$ is not nilpotent. If the minimum equation of $u$ is of degree $n$, the finite sub-algebra $B=(u, u^2, \cdots, u^n)$, of $A$, contains an idempotent element $e=\xi_1 u+\xi_2 u^2+\cdots+\xi_n u^n$, ($\xi_i$ in $\Xi$), (Theorem 1). Hence $[e]=\xi[u]$, $(\xi=\xi_1+\xi_2+\cdots+\xi_n)$. Therefore, $\xi[u]=[e]=[e]^2=\xi^2[u]^2=\xi^2[u]$, and hence $\xi=1$, since $\xi=0$ implies $[e]=[0]$ and $e$ nilpotent. Thus $e$ is an idempotent element of $A$, in class $[u]$ of $A-K$.

THEOREM 9. *If $u$ is a primitive* idempotent element of $A$, and $K$ is a maximal semi-nilpotent invariant sub-algebra of $A$, then $[u]$ is a primitive idempotent element of $A-K$.*

THEOREM 10. *If $e$ is a principal* idempotent element of $A$, then $[e]$ is a principal idempotent element of $A-K$ and is identical with its principal unit.**

Theorem 9 is easily proved by means of Theorems 1 and 8, while Theorem 10 follows readily from Theorems 5 and 6.

* Dickson, pp. 36–40, 55, 49, 15.

THEOREM 11. *If $A$ has the maximal semi-nilpotent invariant sub-algebra $K$, and $A-K$ contains a simple* matric algebra $M$, with an enumerable base, then $A$ contains a sub-algebra equivalent to $M$.*

PROOF. Let $M=[\epsilon_{ij}]$ be a simple matric algebra of classes, in which $[\epsilon_{ij}][\epsilon_{jk}]=[\epsilon_{ik}]$, $[\epsilon_{ij}][\epsilon_{hk}]=[0]$, $(j\neq h,\ i,\ k,\ j,\ h=1,\ 2,\ 3,\ \cdots)$. With $e_{11}$ in $[\epsilon_{11}]$, (Theorem 8), as a basis for induction we shall first prove that $A$ contains idempotent elements $e_{11}, e_{22}, \cdots$ whose products in pairs are zero and such that $e_{ii}$ is in $[\epsilon_{ii}]$.

Let $s=\sum_{i=1}^{n-1}e_{ii}$, where $e_{ii}e_{jj}=0$, $i\neq j$, and $e_{ii}$ is in $[\epsilon_{ii}]$. Let $b_n$ be any element of $A$ in $[\epsilon_{nn}]$ and let $a_n=b_n-sb_n-b_ns+sb_ns$. Then $e_{ii}a_n=0=a_ne_{ii}$, and $[a_n]=[b_n]=[\epsilon_{nn}]$, and hence $[a_n][\epsilon_{ii}]=[0]=[\epsilon_{ii}][a_n]$, $(i=1,\ 2,\ \cdots,\ n-1)$. The sub-algebra $B=(a_n, a_n^2, \cdots, a_n^k)$, of $A$, contains an idempotent element $e_{nn}$ in $[\epsilon_{nn}]$, (Theorem 8), such that $e_{nn}e_{ii}=0=e_{ii}e_{nn}$, $i\neq n$. Therefore $A$ contains idempotent elements $e_{11}, e_{22}, e_{33}, \cdots$ whose products in pairs are zero and such that $e_{ii}$ is in $[\epsilon_{ii}]$ of $M$.

Now consider the non-zero elements $a_{1j}$ and $b_{j1}$ of $A$, in $[\epsilon_{1j}]$ and $[\epsilon_{j1}]$ of $M$, respectively. Let $e_{1j}=e_{11}a_{1j}e_{jj}$, and $a_{j1}=e_{jj}b_{j1}e_{11}$. Then $[e_{1j}]\ [a_{j1}]=[\epsilon_{11}]$ and hence $e_{1j}a_{j1}=e_{11}+k$, ($k$ in $K$, with index $\alpha$). Moreover, $e_{11}\epsilon_{1j}a_{j1}=e_{1j}a_{j1}$, and hence $e_{11}(e_{11}+k)=e_{11}+k$, or $e_{11}k=k$. Similarly, $ke_{11}=k$. Let $e_{j1}=a_{j1}-a_{j1}k+a_jk^2-a_jk^3+\cdots+(-1)^{\alpha-1}a_{j1}k^{\alpha-1}$. Then

$$e_{1j}e_{j1}=(e_{11}+k)-(k+k^2)+\cdots+(-1)^{\alpha-1}(k^{\alpha-1}+k^\alpha)$$
$$=e_{11}+k^\alpha=e_{11}.$$

Similarly, $e_{j1}e_{1j}=e_{jj}+k_1$, ($k_1$ in $K$). Hence from the definitions of $a_{j1}$, $e_{1j}$, and $e_{j1}$, it follows that $e_{jj}k_1=k_1e_{jj}=k_1$. Therefore $(e_{jj}+k_1)^2=e_{jj}+2k_1+k_1^2=(e_{j1}e_{1j})^2=e_{jj}+k_1$, and $k_1^2=-k_1$, from which $k_1^{2\alpha}=-k_1=0$, since $k_1$ is nilpotent. Therefore, $e_{j1}e_{1j}=e_{jj}$.

Let $e_{ij}=e_{i1}e_{1j}$, ($e_{i1}$ in $[\epsilon_{i1}]$, $e_{1j}$ in $[\epsilon_{1j}]$). Then $e_{ij}$ is in $[\epsilon_{ij}]$. From the definitions of $e_{ij}$ and $e_{1j}$ and preceding relations, it follows that

* If $A$ is an algebra of matrices having only a finite number of non-zero elements in each matrix, and if the base elements $(u_k)$, $(k,\ h=1,\ 2,\ \cdots)$, of $A$ are matrices whose elements are all zero except that in the $k$th row and $h$th column, which is unity, then the algebra $M=(\epsilon_{ij})$ equivalent to $A$, in which $(i,\ j)$ have the same range as $(k,\ h)$, will be called a simple matric algebra with the base elements $\epsilon_{ij}$. Thus $\epsilon_{ij}\epsilon_{jk}=\epsilon_{ik}$, $\epsilon_{ij}\epsilon_{hk}=0$, $h\neq j$.

$e_{ij}e_{jl} = e_{ik}$, and $e_{ij}e_{kk} = (e_{i1}e_{1j}e_{jj})(e_{kk}e_{k1}e_{1k}) = 0, \quad j \neq h.$

This completes the proof that $A$ contains elements $e_{ij}$ in classes $[\epsilon_{ij}]$ of $M$, respectively, and such that the elements $e_{ij}$ constitute the base of a sub-algebra of $A$ which is equivalent to $M$.

4. *Canonical Form of the Matrix R.* Every linear associative algebra satisfying the postulates of this paper is equivalent* to a matric algebra, and hence an element of the algebra, and its matric representation, must satisfy the same minimum equation. Every finite matrix can be reduced to a rational canonical† form, but this is not true for matrices of infinite order.

Let $R_a = (\rho_{kj})$ correspond to $a = \sum_i \xi_i u_i$, where $\rho_{kj} = \sum_i \xi_i \gamma_{ijk}$, and $\gamma_{ijk}$ is the coefficient of $u_k$ in the product $u_iu_j$. Since the number of terms $u_k$ in any product $u_iu_j$ is finite, $R_a$ will have but a finite number of non-zero elements in any column. Let $W_i = \sum_k \rho_{ki}u_i$, where $k$ has an infinite range, but only a finite number of the $\rho_{ki}$ are not zero. Let $x_{11} = \sum_i c_i u_i$, and $X_{11} = \sum_i c_i W_i$, be any two corresponding finite linear functions of $u_i$ and $W_i$, respectively, $c_i$ in $\Xi$. Then $X_{11} = \sum_{ik} c_i\rho_{ki}u_k = x_{12}$, and similarly, $X_{12} = \sum_{ik} c_i\rho_{ki}W_k = \sum_{ikh} c_i\rho_{ki}\rho_{hk}u_h = \sum_{ih} c_i\rho'_{hi}u_h = x_{13}$, $X_{13} = \sum_{ik} c_i\rho'_{hi}W_k = \sum_{ij} c_i\rho^{(2)}_{ji}u_j = x_{14}$, etc., where $\rho^{(r-1)}_{kj}$ is the element in the $k$th row and $j$th column of $(\rho_{kj})^r$. These relations may be written more briefly in the form

$$(1) \qquad \begin{aligned} x_{11} &= \sum_i c_i u_i, X_{11} = \sum_{ij} c_i\rho_{ji}u_j = x_{12}, X_{12} = \sum_{ij} c_i\rho'_{ji}u_j = x_{13}, \\ &\cdots, \quad X_{1r} = \sum_{ij} c_i\rho^{(r-1)}_{ji}u_j = x_{1r+1}, \cdots. \end{aligned}$$

If the minimum equation of $a$ is $\lambda^m + \xi_m\lambda^{m-1} + \cdots + \xi_1\lambda + \xi_0 = 0$, then

$$\rho^{(m-1)}_{ji} + \xi_m\rho^{(m-2)}_{ji} + \cdots + \xi_1\rho_{ji} = 0, \ (i \neq j, \ i, j = 1, 2, 3, \cdots),$$
$$\rho^{(m-1)}_{ii} + \xi_m\rho^{(m-2)}_{ii} + \cdots + \xi_1\rho_{ii} + \xi_0 = 0.$$

Therefore

$$X_{1m} + \xi_m X_{1m-1} + \cdots + \xi_1 X_{11} + \xi_0 x_{11} = 0,$$

* M. H. Ingraham, this Bulletin, vol. 32 (1926), p. 589.

† L. E. Dickson, *Modern Algebraic Theories*, p. 89.

which proves the following theorem.

THEOREM 12. *If $(\rho_{kj})$ satisfies an equation of degree $m$, with rational coefficients, the number of linearly independent linear functions $x_{11}, X_{11}, \cdots, X_{1i-1}$, as determined in* (1), *is $\alpha \leqq m$.*

In what follows we shall write (1) in the form

$$X_{11} = x_{12}, \quad X_{12} = x_{13}, \cdots, \quad X_{1\alpha-1} = x_{1\alpha},$$

$$X_{1\alpha} = \sum_{i=1}^{\alpha} \xi_{1i} x_{1i} = [x_{11}, \cdots, x_{1\alpha}]. \tag{1'}$$

Any finite linear expression $\sum_i c_i u_i$ leads to a chain of the type of (1'). The maximal length of all such chains is $\alpha_1 \leqq m$.

THEOREM 13. *If $R_a = (\rho_{kj})$ corresponds to the element $a = \sum_i c_i u_i$ of a rational linear associative algebra $A$, with the enumerable base $(u_1, u_2, u_3, \cdots)$, then $R_a$ may be reduced to a canonical form defined by*

$$X_{i_i 1} = x_{i_i 2}, \cdots, \quad X_{i_i \alpha_i - 1} = x_{i_i \alpha_i},$$

$$X_{i_i \alpha_i} = [x_{i_i 1}, x_{i_i 2}, \cdots, x_{i_i \alpha_i}], \tag{2}$$

$$(i = 1, 2, \cdots, p \leqq \alpha_1; j_i = 1, 2, 3, \cdots),$$

*in which $X_{j_i 1}, X_{j_i 2}, \cdots, X_{j_i \alpha_i}$ are the elements of the $j_i$th chain of length $\alpha_i$, each of which is linearly independent of all preceding chains of length $\alpha_1, \alpha_2, \cdots, \alpha_{i-1}$ and the preceding elements of the $j_i$th chain of length $\alpha_i$. Moreover, $\alpha_1$ is the maximal length of all possible chains, and in general, $\alpha_i$ is the maximal length of all chains of length less than $\alpha_{i-1}$ which are linearly independent of all chains of length $\alpha_1, \alpha_2, \cdots, \alpha_{i-1}$.*

Proofs of this theorem for the finite case that have been given by L. E. Dickson (*Modern Algebraic Theories*, p. 90), or M. H. Ingraham (this Bulletin, vol. 39, p. 379), may be extended to the infinite case, provided we secure the leaders of successive chains as follows.

The leader, $x_{11} = \sum_i c_i u_i$, of the first chain of length $\alpha_1$ may be obtained from successive trials of the linear functions $\sum_i c_i u_i$ such that $\sum i = n$, $(n = 1, 2, \cdots, k_1)$. The leaders of the succeeding chains of length $\alpha_1$ may be obtained in the same way with $\sum i = n$, $(n = k_1, k_1+1, k_1+2, \cdots, k_2; k_2, k_2+1, \cdots, k_3;$ etc.). To obtain the chains of length $\alpha_2, \alpha_3$, etc., repeat the entire

process for $\alpha_2$, then for $\alpha_3$, etc. With (1′) as a basis for induction we can prove that the $k$th chain of length $\alpha_1$ can be expressed in the form

$$(3)\quad X_{k1} = x_{k2}, \cdots, \quad X_{k\alpha_1-1} = x_{k\alpha_1}, \quad X_{k\alpha_1} = [x_{k1}, x_{k2}, \cdots, x_{k\alpha_1}].$$

Similarly, all chains of length $\alpha_i$ can be reduced to forms of the type of (3). We can thus reduce $(\rho_{kj})$ to the canonical form defined by (2), in which there are infinitely many partial transformations, but not more than $\alpha_1$ different lengths to the chains.

Each of the base elements $u_1, u_2, u_3, \cdots$, either is itself an element of (2), or else is a finite linear combination of such elements. For, in the process of determining the complete canonical transformation, any $u_i$ which is finitely linearly independent of all previously determined $x_{jk}$ is taken as the leader of a new chain and is therefore itself an $x_{jk}$. Hence it is possible to determine uniquely each of the variables $u_i$ in terms of the variables $x_{jk}$.

The characteristic determinant of the matrix of any chain is divisible by that of any other chain of equal or lower order. Hence the minimum function of $(\rho_{kj})$ is identical with that of the chain of maximal length, and if $(\rho_{kj})$ satisfies no finite equation it cannot be reduced to a rational canonical form with a chain of maximal length $\alpha$.

BELOIT COLLEGE

# THE APPARENT CONTOUR OF THE GENERAL $V_3^n$ IN $S_4$*

BY A. R. WILLIAMS

It is the purpose of this paper to study the surface obtained by intersecting with a 3-space the hypercone of tangents drawn to a hypersurface $V$ in $S_4$ from a point $O$. Or we may say that we project from $O$ upon $S_3$ the surface which is the intersection of $V$ and the first polar hypersurface of $O$. It may be recalled that when $V$ is the locus of lines that meet four planes, and therefore a fifth, and $O$ is a general point of $V$, the Kummer surface is the result. In this paper $V$ will be assumed non-singular and of order $n$. But the surface obtained has all the ordinary singularities, including a cuspidal curve. The two cases when the center of projection is not a point of $V$, and when it is on $V$, will be considered in that order.

If $V$ is a non-singular hypersurface in $S_4$ of order $n$, and $O$ any point not on $V$, the hypercone of tangents to $V$ from $O$ meets a 3-space in a surface $F'$ of order $n(n-1)$. For a line in $S_3$ determines with $O$ a plane that meets $V$ in a curve to which $n(n-1)$ tangents can be drawn from $O$. As remarked, $F'$ is the projection from $O$ of the surface $F$, which is the intersection of $V$ and the first polar hypersurface of $O$. The second polar hypersurface of $O$ meets $F$ in a curve $C$ of order $n(n-1)(n-2)$ whose projection is the cuspidal curve of $F'$. For, if $P$ is a general point of $C$, the tangent plane to $F$ at $P$ passes through $O$. A 3-space containing $OP$, but not the tangent plane, meets $F$ in a curve to which $OP$ is a simple tangent. Hence its projection is a plane curve on $F'$, having a cusp at $P'$, the projection of $P$. The cuspidal tangent is the intersection with $S_3$ of the osculating plane to the space curve at $P$. As the 3-space section through $OP$ varies there are $\infty^1$ distinct osculating planes. They lie in the 3-space which is tangent to $V$ at $P$. For this 3-space intersects $V$ in a surface having a node at $P$, and intersects the first polar of $O$ in a surface whose tangent plane at $P$ is the tangent plane to $F$. The second of these surfaces is the polar of $O$ with respect to the first. Furthermore, $OP$ meets $V$ in three points at $P$. From all of which

* Presented to the Society, December 2, 1933.

it follows that the tangent plane to $F$ at $P$ is tangent along $OP$ to the quadric cone of lines that meet $V$ three times at $P$, and that the 3-space in question intersects $F$ in a curve having a cusp at $P$, whose cuspidal tangent is $OP$. The tangent plane to $F$ is the osculating plane to this curve and meets it, and therefore $F$, in four points at $P$. Therefore this 3-space, tangent to $V$ at $P$, meets $S_3$ in a plane $\pi$, which contains the cuspidal tangents to all sections of $F'$ by planes through $P'$. The plane $\pi$ meets $F'$ in a curve having a triple point, whose only real tangent is the tangent to the cuspidal curve, that is, the intersection with $S_3$ of the tangent plane to $F$ at $P$. A general 3-space of the pencil that contains the tangent plane to $F$ at $P$ meets $V$ in a surface to which that plane is a stationary tangent plane, and meets $F$ in a curve which has a double point at $P$. The projections of these curves give the pencil of plane sections of $F'$ whose axis is the tangent to the cuspidal curve. Such a section has a tacnode at $P'$ instead of a cusp. The order of the cuspidal curve is called $c$. Thus we have $c=n(n-1)(n-2)$.

To find the double curve and the triple points, let $Q'$ with coordinates $(x_1' : x_2' : x_3' : x_4' : x_5')$ be a point of $V$, and $Q(x_1 : x_2 : x_3 : x_4 : x_5)$ a general point of $S_4$. Then the coordinates of a point on $Q'Q$ are $x_i' + \lambda x_i$, $(i=1, 2, \cdots, 5)$. We suppose that $Q'Q$ meets $V$ in two points at $Q'$, and we require that it be tangent to $V$ elsewhere. This means the vanishing of the discriminant of the residual equation in $\lambda$ of order $n-2$. This discriminant is of order $n(n-1)-6$ in the coordinates of $Q$, and combined with the tangent 3-space at $Q'$ represents the cone of lines tangent to $V$ at $Q'$ and once elsewhere. The same discriminant is of order $(n-2)(n-3)$ in the coordinates of $Q'$. Hence if $Q$, or $O$, is a fixed point, not on $V$, the points of contact of the double tangents to $V$ from $O$ lie on a hypersurface of order $(n-2)(n-3)$. They lie also on the surface $F$, and hence fill a curve $B$ of order $n(n-1)(n-2)(n-3)$, which lies on a cone of half that order with vertex at $O$. This cone meets $S_3$ in the double curve of $F'$, whose order is therefore $\frac{1}{2}n(n-1)(n-2)(n-3)$. The order of the double curve is called $b$.

To find the triple points we require that the above equation of order $n-2$ in $\lambda$ have two distinct pairs of equal roots. We thus get a restricted system, whose order is $4n(n-4)(n-5) + \frac{1}{2}(n-2)(n-3)(n-4)(n-5)$ or $\frac{1}{2}(n-4)(n-5)(n^2+3n+6)$ in the coordinates of $Q$, and is $\frac{1}{2}(n-2)(n-3)(n-4)(n-5)$ in the

coordinates of $Q'$.* This means that, from a point $Q'$ on $V$, $\frac{1}{2}(n-4)(n-5)(n^2+3n+6)$ lines can be drawn tangent to $V$ at $Q'$ and twice elsewhere. If $Q$, or $O$, is a point not on $V$ it means that the number of points of contact of lines drawn from $O$ tangent three times to $V$ is $\frac{1}{2}n(n-1)(n-2)(n-3)(n-4)(n-5)$; and hence the number of triple tangents to the hypersurface $V$ from $O$, or the number of triple points on the double curve of $F'$ is $\frac{1}{6}n(n-1)(n-2)(n-3)(n-4)(n-5)$. The number of these points, which are triple on the double curve and triple on the surface, is denoted by $t$.

To find the intersections of the double and cuspidal curves we note first that their originals $B$ and $C$ in $S_4$ do not in general have an apparent double point as seen from $O$. For that would demand that a line through $O$ satisfy four conditions. But the curves $B$ and $C$ do meet on $F$ where the second polar hypersurface of $O$ meets $B$. These intersections of the curves $B$ and $C$ are of two sorts. First there are the $n(n-1)(n-2)(n-3)$ points common to $V$ and the first three polar hypersurfaces of $O$. At such a point, $B$ and $C$ are tangent. Hence the number of remaining intersections is $n(n-1)(n-2)^2(n-3)-2n(n-1)(n-2)(n-3)$ $=n(n-1)(n-2)(n-3)(n-4)$. If $P$ is a point of the first sort, $OP$ meets $V$ four times at $P$ and the first polar of $O$, and therefore $F$, three times. Also $OP$ is a simple tangent to $C$, and therefore the cuspidal curve of $F'$ has itself a cusp at $P'$. The line $OP$ is tangent to $B$ at $P$; but since $B$ meets twice each generator of the projecting cone, $P'$ is not a cusp of the double curve, but a point where it changes from crunodal to acnodal. Now a general 3-space containing $OP$, but not the tangent plane to $F$, meets $F$ in a curve to which $OP$ is an inflectional tangent. Therefore its projection is a plane curve for which $P'$ is not a cusp, but a triple point with one real tangent. These tangents form a plane pencil as before. Now the tangent plane to $F$ at $P$ meets $F$ in six points there. A general 3-space containing this plane meets $F$ in a curve having a double point $P$, one of whose tangents is $OP$; and the tangent 3-space to $V$ meets $F$ in a curve having a tacnode whose tangent is $OP$. Again if $P$ is an intersection of $B$ and $C$ of the second sort, $OP$ will meet $V$ three times at $P$ and be tangent to $V$ at one other point. The point $P'$ will be a point of $F'$ where the cuspidal curve is intersected by a sheet

* Salmon: *Higher Algebra*, §278.

belonging to the double curve, and will be a cusp of the double curve. The number of intersections of the cuspidal curve and double curve which are cusps on the former is called $\beta$, and the number that are cusps on the latter is called $\gamma$. From what precedes, therefore, we see that $\beta = n(n-1)(n-2)(n-3)$ and $\gamma = n(n-1)(n-2)(n-3)(n-4)$.

We now consider the tangent cone to $F'$ from a general point $O'$ of $S_3$. The first polar hypersurface of $O'$ meets $F$ in a curve $A$, the intersection of $V$ and the first polars of $O$ and $O'$. At a point $P$ of $A$ the tangent 3-space to $V$ passes through $O$ and $O'$, and meets $F$ in a curve with a double point at $P$, whose projection lies in a plane through $O'$ tangent to $F'$ at $P'$. Thus the order $a$ of the tangent cone to $F'$ is $n(n-1)^2$. The class of that cone, or class of $F'$, is the number of 3-spaces through a plane $OO'O''$ tangent to $V$. It is denoted by $n'$ and is $n(n-1)^3$. The number $\Delta$ of planes through a line that meet twice the curve $A$, whose projection is the curve of contact, is given by

$$2\Delta = n(n-1)^2[n(n-1)^2 - 3n + 4] = n(n-1)^2(n-2)(n^2-2).$$

Hence to find $\kappa$ and $\delta$, the number of cuspidal and double edges of the tangent cone, we have

$$2(\kappa + \delta) = n(n-1)^2(n-2)(n^2-2)$$

and

$$n(n-1)^2[n(n-1)^2 - 1] - 2\delta - 3\kappa = n(n-1)^3.$$

Hence $\kappa = 2n(n-1)^2(n-2)$ and $\delta = \frac{1}{2}n(n-1)^2(n-2)(n^2-6)$. The intersections of the curve of contact with the double curve and cuspidal curve correspond to the intersections of $A$ with $B$ and $C$, and are $n(n-1)^2(n-2)(n-3)$ and $n(n-1)^2(n-2)$ in number. These numbers which give the class of the nodal developable and that of the cuspidal developable are called $\rho$ and $\sigma$, respectively. For the curve $C$, we have as above

$$2\Delta = n(n-1)(n-2)[n(n-1)(n-2) - 3(n-3) + 2].$$

Dividing by 2 and subtracting the $\beta$ cusps, we obtain $h$, the number of apparent double points of the cuspidal curve. Thus $h = \frac{1}{2}n(n-1)(n-2)[n^3-3n^2-3n+11]$. To find $k$, the number of apparent double points of the double curve, we find two expressions for the rank, or class, of $B$, one of which involves $k$. The order of the hypersurface which meets $B$ in the points where the

tangent meets a given plane is $n-1+n-2+(n-2)(n-3)-1$, or $(n-1)(n-2)$. Now the three points of contact on one of the triple tangents to $V$ from $O$ are double points of $B$. For such a tangent is a triple generator of the cone that projects $B$ from $O$, and therefore a general three-space containing it meets $B$ in $n(n-1)(n-2)(n-3)-6$ other points. Also if $P_1$ is a point on $\gamma$, $OP_1$ is tangent to $B$ at $P_1$ and meets $B$ again at $P_2$, where $B$ is not tangent to the generator, but has a cusp. Hence the rank of $B$ is $n(n-1)^2(n-2)^2(n-3)-6t-3\gamma$. Again if we take an arbitrary plane through $O$, the rank of $B$ is given by $\beta+\gamma$, the number of tangents to $B$ that pass through $O$, plus the number of tangents to $B$ that meet the arbitrary plane elsewhere. Since a general generator of the cone meets $B$ twice, the latter number is twice the rank of the cone, that is, twice the rank of the double curve of $F'$. Hence we have the equation

$$n(n-1)^2(n-2)^2(n-3) - 6t - 3\gamma = \beta + \gamma + 2[N(N-1) - 2k - 3\gamma - 6t],$$

where $N=\frac{1}{2}n(n-1)(n-2)(n-3)$, the order of the double curve. Hence

$$k = n(n-1)(n-2)(n-3)[n^4 - 6n^3 + 7n^2 + 14n - 28]/8.$$

We may summarize what precedes as follows. When $V$ is of order $n$ and the center of projection is not on $V$, the order of $F'$, the surface obtained in $S_3$, is $n(n-1)$. The orders, $c$ and $b$, of its cuspidal and double curves are $n(n-1)(n-2)$ and $\frac{1}{2}n(n-1)(n-2)(n-3)$. The numbers, $\beta$ and $\gamma$, of intersections of the two curves which are cusps on the former and latter, respectively, are

$$n(n-1)(n-2)(n-3) \quad \text{and} \quad n(n-1)(n-2)(n-3)(n-4).$$

The number, $t$, of points triple on the double curve and triple on $F'$ is $n(n-1)(n-2)(n-3)(n-4)(n-5)/6$. The order, $a$, of a general tangent cone is $n(n-1)^2$. Its class, $n'$, or the class of $F'$, is $n(n-1)^3$. The numbers, $\sigma$ and $\rho$, of intersections of the curve of contact with the cuspidal and double curves are $n(n-1)^2(n-2)$ and $n(n-1)^2(n-2)(n-3)$. The numbers, $\kappa$ and $\delta$, of cuspidal and double edges of the tangent cone are $2n(n-1)^2(n-2)$ and $\frac{1}{2}n(n-1)^2(n-2)(n^2-6)$. The numbers, $h$ and $k$, of apparent double points of the cuspidal and double

curves were given in the last paragraph. There are apparently no close points on the cuspidal curve, nor points at which the cuspidal and double curves meet but which are singular on neither. It will be found that the above results satisfy identically the established formulas for surfaces in $S_3$; see, for example, Salmon's *Solid Geometry*, 5th edition, the six equations A and B, §§610 and 612. In those equations $n$, which denotes the order of the surface, must be replaced by $n(n-1)$.

The Hessian of $V$ meets the surface $F$ in a curve $H$ of order $5n(n-1)(n-2)$ whose projection is the parabolic curve of $F'$. At a point of $H$ the quadric cone of lines that meet $V$ three times there becomes two planes, and the tangent 3-space to $V$ meets $F$ in a curve having a cusp. The Hessian meets the curve $A$ in $5n(n-1)^2(n-2)$ points. This number is the class of the spinode torse of $F'$. The Hessian meets $C$ in $5n(n-1)(n-2)^2$ points. At such a point one of the pair of planes just mentioned passes through $O$ and is the tangent plane to $F$. The tangent three-space to $V$ meets $C$ three times there. Hence at the projected point, where the parabolic curve of $F'$ meets the cuspidal curve, the osculating plane to the latter is the tangent plane to the surface. Applying Plücker's equations to the tangent cone, we find the class of the bitangential developable to be

$$\tfrac{1}{2}n(n-1)^2(n-2)(n^4-2n^3+2n^2-15).$$

We infer that the bitangential curve is the projection of a curve on $F$ in $S_4$ of order $n(n-1)(n-2)(n^4-2n^3+2n^2-15)$. This number is checked by use of the formulas for surfaces in $S_3$. It appears also that the locus of points of contact of 3-spaces doubly tangent to $V$ is the intersection of $V$ with a hypersurface of order $(n-2)(n^4-2n^3+2n^2-15)$; this might be proved otherwise.

It remains to indicate briefly the modifications to be made when the center of projection $O$ is a point of $V$. Now the polar hypersurfaces of $O$ have in common the tangent 3-space, the quadric cone of lines that meet $V$ three times at $O$, and the six lines that meet it four times. The order of $F$ is the same; but the order of $F'$ is $n(n-1)-2$. The curve $C$, the intersection of $V$ with the first two polars of $O$, has a sextuple point at $O$, the tangents being the six lines that meet $V$ four times there. This curve is met by a general 3-space in six points at $O$, but by the tangent 3-space in 24. Thus $c$, the order of the cuspidal curve

of $F'$, is $n(n-1)(n-2)-6$. A general 3-space through $O$ meets $F$ in a curve having a double point there. The cone projecting this curve from $O$ has $\frac{1}{2}n(n-1)(n-2)(n-3)-3[n(n-1)-6]$ double edges. This is the number $b$, the order of the double curve of $F'$. It is the previous value diminished by two for each line that can be drawn (in the 3-space section) tangent to $V$ at $O$ and once elsewhere. Now

$$2b = n(n-1)[(n-2)(n-3)-2]-2(n-4)(n+3).$$

This suggests that the points of contact of the double tangents to $V$ from $O$ lie on a hypersurface of order $(n-2)(n-3)-2$, and fill a curve $B$ of order $n(n-1)[(n-2)(n-3)-2]$ on $F$ that has a multiple point of order $2(n-4)(n+3)$ at $O$. This is seen by the method used for the similar problem above. If $Q$, or $O$, is on $V$, the coefficient of the highest power of $\lambda$ in the equation of order $n-2$ vanishes and the discriminant is divisible by the square of the preceding coefficient, which, when the primed letters are variable, represents the three-space tangent to $V$ at $O$. With regard to the multiple point of the curve at $O$, we note that the quadric cone of lines meeting $V$ three times at $O$ and the residual cone of order $n(n-1)-6$ are tangent along the six lines that meet $V$ four times at $O$, and hence have in common $2(n-4)(n+3)$ other generators. Such a generator meets $V$ three times at $O$, and is tangent to $V$ elsewhere. It is evidently a generator of the cone of double tangents drawn to $V$ from $O$. The quadric cone of lines that meet $V$ three times at $O$ gives on the surface $F'$ a trope, that is, a conic whose plane is tangent to $F'$ along the conic. The residual cone at $O$, in the tangent 3-space, has $n(n-1)(n-2)-24$ cuspidal edges, and $\frac{1}{2}(n-4)(n-5)(n^2+3n+6)$ double edges, that is, lines tangent to $V$ at $O$ and twice elsewhere. Hence the cuspidal curve on $F'$ meets the plane of the trope three times where each of the six lines meets it; and the double curve is tangent to the plane of the trope where each of the $2(n-4)(n+3)$ generators meets it. For the difference between the number of double tangents that can be drawn to $V$ from $O$ in a general 3-space and in the tangent 3-space is $4(n-4)(n+3)$. The number, $\beta$, of points common to $V$ and the first three polars of $O$ is $n(n-1)(n-2)(n-3)-24$. The second polar of $O$ meets $B$ $3\cdot 2(n-4)(n+3)$ times at $O$, and hence

$$\gamma = n(n-1)(n-2)[(n-2)(n-3)-2]-6(n-4)(n+3)$$
$$-2[n(n-1)(n-2)(n-3)-24]$$
$$= n(n-1)(n-2)(n-3)(n-4)-2(n-4)(n^2+4n+15).$$

The order and class of the general tangent cone to $F'$ and its other characteristics remain as before. The number $\sigma$ is the same; but $\rho$ is $n(n-1)^2[(n-2)(n-3)-2]$, that is, reduced by $2n(n-1)^2$. We can infer also that the number of triple tangents to $V$ from $O$ is the number in the previous case diminished by two for each of the $\frac{1}{2}(n-4)(n-5)(n^2+3n+6)$ lines that can be drawn tangent to the hypersurface $V$ at $O$ and twice elsewhere. Thus the number of triple points is found to be $(n-4)(n-5)(n-6)(n+1)(n^2-n+6)/6$; a result which can be checked by the relation $b(n-2)=\rho+2\beta+3\gamma+3t$, on replacing $n$ by $n(n-1)-2$. To find $h$, the number of apparent double points of the cuspidal curve, we note that the rank of $C$ is reduced by 18 by the sextuple point at $O$. For, taking the origin at $O$, we easily see that the hypersurface which meets $C$ in the points where the tangent meets a given plane has a triple point at $O$. Thus the rank of $C$ is $3n(n-1)(n-2)^2-18$. But the rank of $C$ is the number $\beta$ of tangents to $C$ from $O$, plus the six tangents at $O$ taken twice, plus the rank of the cone projecting $C$, that is, the rank of the cuspidal curve. Hence we have $3n(n-1)(n-2)^2-18=\beta+12+M(M-1)-2h-3\beta$, where $M=n(n-1)(n-2)-6$. Hence we shall have also the relation $k=\frac{1}{2}n(n-1)(n-2)[n^3-3n^2-3n-1]+60$. It would be possible, but too tedious, to make the corresponding modification for $B$, and so find $k$ independently.

Finally it must not be forgotten that some of the statements in the last paragraph require obvious modification when $n=3$. Thus when $O$ is a point of a general cubic hypersurface we get a quartic surface in $S_3$ with no double or cuspidal curve, but having a trope on which are six nodes, the points in which its plane is met by the six lines through $O$ that lie on $V$ and on $F$. For a plane through one of them meets $V$ in a conic to which two tangents can be drawn from $O$. The order and class of the tangent cone are as above $n(n-1)^2$ and $n(n-1)^3$, that is, 12 and 24. Similarly for its other characteristics. The trope is the 16th trope of the Kummer surface obtained when the cubic hypersurface is of the sort mentioned in the introduction to this paper.

THE UNIVERSITY OF CALIFORNIA

# ON POWER CHARACTERS IN CYCLOTOMIC FIELDS

BY H. S. VANDIVER

1. *Introduction.* In a previous paper,* I considered power characters in the field $K(\zeta)$; $\zeta = e^{2i\pi/l}$, where $l$ is an odd prime. We write

$$\omega^{(N(\mathfrak{p})-1)/l} \equiv \zeta^a \pmod{\mathfrak{p}},$$

where $\omega$ is an integer in $K(\zeta)$; $\mathfrak{p}$ is an ideal in that field with $\omega$ and $\mathfrak{p}$ prime to $l$. Moreover,

$$\{\omega/\mathfrak{p}\} = \left\{\frac{\omega}{\mathfrak{p}}\right\} = \zeta^a$$

in the case where the field $K(\zeta)$ is properly irregular, that is, when the second factor of the class number of $K(\zeta)$ is prime to $l$. An explicit algebraic expression was found for $a$ in the above relation provided $\omega$ was a unit in the field. This expression had been well known in the case where $\mathfrak{p}$ belonged to an exponent prime to $l$. In the same paper (pp. 400–401) an explicit expression was found for the symbol $\{\theta/\mathfrak{q}\}$, where $\theta$ is an integer and $\mathfrak{q}$ is a prime ideal in $K(\zeta)$ prime to $l$; also $\theta = \mathfrak{a}^l$, where $\mathfrak{a}$ is a prime ideal in the same field. These ideas appear quite novel in this connection and they possibly constitute the germs of an extension of the theory of relative abelian fields.

One aspect of the matter is the following. If $\theta = \alpha^l$, then we have the trivial conclusion that

$$\{\theta/\mathfrak{q}\} = 1.$$

The result we have been discussing is an extension of the one just mentioned since $\theta$ is the $l$th power of an ideal which is not necessarily principal. The value of the power characters involving $\theta$ depended upon those involving $\omega$, where $\omega$ is a unit, and these in turn depended upon the following relation due to Kummer:

$$(1)\quad \operatorname{ind} E_n \equiv \frac{r^{2n}-1}{2(1+a^{l-2n}-(a+1)^{l-2n})} \cdot \frac{d_0^{l-2n} \log \psi_a(e^v)}{dv^{l-2n}} \pmod{l},$$

* Transactions of this Society, vol. 32 (1930), pp. 391–408.

where

$$\left\{\frac{E_n}{\mathfrak{q}}\right\} = \zeta^{\operatorname{ind} E_n},$$

$a$ is a rational integer, $0<a<l-1$, $r$ is a primitive root of $l$,

$$\psi_a(x) = \sum_h x^{-(a+1)h+\operatorname{ind}(g^h+1)},$$

$x$ is arbitrary, $\mathfrak{q}$ is an ideal prime in $k(\zeta)$ whose norm is $q^t$, $g$ is a primitive root of $\mathfrak{q}$, $h$ ranges over the integers $0, 1, 2, \cdots, q^t-2$, excepting $(q^t-1)/2$ if $q$ is odd and excepting zero if $q$ is even. The primitive root $g$ is selected so that

$$g^{(q^t-1)/l} \equiv \zeta \pmod{\mathfrak{q}}.$$

If

$$g^h + 1 \equiv g^k \pmod{\mathfrak{q}},$$

$0<k<q^t-1$, then we write

$$\operatorname{ind}(g^h + 1) = k.$$

The symbol

$$\frac{d_0^{l-2n} \log \psi_a(e^v)}{dv^{l-2n}}$$

means that the $(l-2n)$th derivative of $\log \psi_a(e^v)$ is taken with respect to $v$ and $v=0$ substituted in the result, $e$ being the Napierian base. Further $a$ is selected so that

$$1 + a^{l-2n} - (a+1)^{l-2n}$$

is prime to $l$. Also

$$E_n = \epsilon^R,$$

$$R = (1 + sr^{-2n} + s^2r^{-4n} + \cdots + s^{(l-3)/2}r^{-n(l-3)})r^l,$$

the symbol $s$ representing the substitution $(\zeta/\zeta^r)$ in the notation of the Kronecker-Hilbert symbolic powers, $r$ is a primitive root of $l$, and

$$\epsilon = \left(\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}\right)^{1/2}.$$

The writer* extended (1) to the case of $l$th power characters in a field defined by $(ln)$th roots of unity, $n$ prime to $l$.

In the present paper several different types of extensions of the above results will be considered. The proofs, in the main, will be indicated only.

2. *Power Characters.* In the first place, if $n$ is an odd prime distinct from $l$ and

$$\beta = e^{2i\pi/n},$$

then we may consider $\{\omega/\mathfrak{A}\}$, where

$$\omega = \frac{1-\beta^l}{1-\beta}.$$

To find expressions involving this power character we employ the Lagrange resolvent form

$$\begin{aligned} F(u, x) &= \eta + u\eta_1 + u^2\eta_2 + \cdots + u^{\lambda-1}\eta_{\lambda-1}, \\ \lambda &= ln, \\ \eta_k &= x^{g^k} + x^{g^{\lambda+k}} + \cdots + x^{g^{(\nu-1)\lambda+k}}, \end{aligned}$$

where $q$ is the norm of $\mathfrak{q}$ in $k(\alpha\beta)$ and a prime of the form $ln\nu+1$, $x^q=1$, $x\neq 1$, and $g$ is a primitive root of $q$. Consider $F(u, x)F(u^{-1}, x)$, where $u$ is arbitrary. We find

$$F(u, x)\,F(u^{-1}, x) = -V\frac{u^\lambda - 1}{u-1} + q + X_1(u^\lambda - 1),$$

where $X_1$ is a polynomial in $u$ with integral coefficients. We set $u=\beta e^v$ in the above expression. By a method analogous to that employed previously by the writer (loc. cit., p. 143), we have

$$\begin{aligned} \frac{d_0^l \log F(e^v\beta, x)}{dv^l} &\equiv f_l(\beta)f_0(\beta^{-1}) - (l-1)f_{l-1}(\beta)f_1(\beta^{-1}) \\ &\quad + \cdots + f_1(\beta)f_{l-1}(\beta^{-1}) \pmod{l}, \end{aligned}$$

where

$$f_s(\beta) = \eta_1\beta + 2^s\eta_2\beta^2 + \cdots + (\lambda-1)^s\eta_{\lambda-1}\beta^{\lambda-1}.$$

* American Journal of Mathematics, vol. 47 (1925), pp. 140–147.

The right-hand expression may then be written in the form

$$\sum_{i=0}^{\lambda-1}\sum_{k=0}^{\lambda-1}\beta^{i-k}i(k-1)^{l-1}\eta_i\eta_k.$$

Writing $k$ for $k-1$, we obtain

$$(2)\qquad \begin{aligned} s &= \sum_{e=1}^{n-1}\frac{d_0{}^l \log F(e^v, \beta^e x)}{dv^l} \\ &\equiv \sum_{e=1}^{n-1}\sum_{i=0}^{\lambda-1}\sum_{k=0}^{\lambda-1}\beta^{-ke}ik^{l-1}\eta_i\eta_{k+1}. \end{aligned}$$

By a method similar to that used by Kummer,* we find

$$(3)\qquad s \equiv n(n-1)I(l) \pmod{l},$$

where

$$\left\{\frac{\theta}{\mathfrak{q}}\right\} = \zeta^{I(\theta)}.$$

From (2) we also have

$$(4)\qquad \begin{aligned} s_1 &= \sum_{e=1}^{n-1}\beta^{ce}\frac{d_0{}^l \log F(e^v, \beta^e x)}{dv^l} \\ &\equiv \sum_{e}\sum_{i}\sum_{k}\beta^{(-k+c)e}ik^{l-1}\eta_i\eta_{k+1}, \end{aligned}$$

which gives, after some transformations,

$$(5)\qquad s_1 \equiv I\left(\frac{1-\beta^{cl}}{1-\beta^c}\right) - \frac{1}{n}I(l) \pmod{l}.$$

From (2), (3), (4), and (5), we have the relations from which we can derive expressions involving $\sigma$, where $\mathfrak{q}^{l^n-1} = (\sigma)$, by factoring the Lagrange resolvent into its prime factors, as did Kummer,† and proceeding as in the writer's paper. Similarly, by these methods we may find analogous expressions for the power characters of certain units with respect to $\mathfrak{p}$ from other relations given by the writer.

---

* Journal für Mathematik, vol. 44 (1851), p. 100.

† Loc. cit., p. 103.

3. *Extensions.* We shall now indicate how to obtain an extension of (1) for $l^n$th power characters. If $\theta$ is an integer in the field $K(\zeta_n)$, where

$$\zeta_n = e^{2i\pi/l^n},$$

which is prime to $1-\zeta_n$, and $\mathfrak{p}$ is an ideal in $K(\zeta_n)$ prime to $\theta$, then

$$\theta^{(N(\mathfrak{p})-1)/l^n} \equiv \left\{\frac{\theta}{\mathfrak{p}}\right\}_n \pmod{\mathfrak{p}},$$

where $\{\theta/\mathfrak{p}\}_n$ is a power of $(\zeta_n)$ and $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$ in $k(\zeta_n)$. To effect this we extend the methods of Kummer.* Set $\lambda = l^n$, and write

$$\psi_r(\zeta) = \sum \zeta^{-(n+1)h + \operatorname{ind}(g^h+1)},$$
$$r+1 \not\equiv 0 \pmod{\lambda}, \qquad r \not\equiv 0 \pmod{\lambda},$$

where the summation extends over the values $h = 0, 1, 2, \cdots, q^t-2$, with the exception

$$\frac{q^t-1}{2}$$

if $q$ is odd and zero if $q$ is even, $q$ being a prime such that $q$ belongs to the exponent $t$ modulo $\lambda$. Further, $g$ is a primitive root of $\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal factor of $q$ which is selected so that

$$g^{(q^t-1)/\lambda} \equiv \zeta_n \pmod{\mathfrak{q}}.$$

The symbol ind $(g^h+1)$ stands for an integer $k$ in the relation

$$(g^h+1) \equiv g^k \pmod{\mathfrak{q}}.$$

This function has the property proved by Mitchell:†

$$\psi_r(\zeta)\psi_r(\zeta^{-1}) = q^t.$$

The method of proof employed there shows that in lieu of the above relation we may write an identity in the form

$$\psi_r(x)\psi_r(x^{l-1}) = q^t + V(x)W(x), \tag{6}$$

where $V(x) = 1+x+x^2+\cdots+x^{\lambda-1}$. Consider

* Loc. cit., p. 103.

† Transactions of this Society, vol. 17 (1916), pp. 165–177.

$$\frac{d^{m+1}\log\psi_r(e^v)}{dv^{m+1}} = \frac{d^m\left(\frac{d\psi_r(e^v)}{dv}\cdot\frac{1}{\psi_r(e^v)}\right)}{dv^m}.$$

If we set

$$\frac{1}{\psi_r(e^v)} = u,$$

then we have by Leibnitz's theorem

$$(7)\qquad \frac{d^{m+1}\log\psi_r(e^v)}{dv^{m+1}} = \frac{d^{m+1}\psi_r(e^v)}{dv^{m+1}}u + \frac{m}{1}\frac{d^m\psi_r(e^v)}{dv^m}\frac{du}{dv} + \cdots.$$

Now set $x=e^v$ in (6). We have

$$\frac{d^i\psi_r(e^{-v})}{dv^i} = \frac{d^iu}{dv^i}(q^i + VW) + \frac{i}{1}\frac{d^{i-1}u}{dv^{i-1}}\frac{d(VW)}{dv} + \cdots.$$

Set $v=0$ in this relation. Then $V$ and all its derivatives except those of orders which are multiples of $l-1$ are divisible by $\lambda$.

By a special treatment of the derivatives of orders which are multiples of $(l-1)$ of $(VW)$ we obtain from the last relation

$$\frac{d_0^iu}{dv^i} \equiv (-1)^i\frac{d_0^i\psi_r(e^v)}{dv^i} \equiv (-1)^iD_i \pmod{\lambda},$$

from which

$$\frac{d_0^{m+1}\log\psi_r(e^v)}{dv^{m+1}} \equiv D_{m+1}D_0 - \frac{m}{1}D_mD_1 + \frac{m(m-1)}{1\cdot 2}D_{m-1}D_2 - \cdots, \pmod{\lambda}.$$

Proceeding as Kummer* did in the special case, we obtain

$$(8)\qquad \frac{d_0^{m+1}\log\psi_r(e^v)}{dv^{m+1}} \equiv (1 + r^{m+1} - (r+1)^{m+1}) \cdot \sum_h h^m \operatorname{ind}(g^h - 1) \pmod{\lambda}$$

* Loc. cit., pp. 125–130.

for $h=1, 2, 3, \cdots, q^t-2$. The right-hand member of this may be transformed into an expression involving units in the field $k(\zeta_n)$ if we note that

$$\sum_h h^m \operatorname{ind}(g^h - 1) \equiv \sum_i \sum_k i^m \operatorname{ind}(g^{i+k\lambda} - 1)$$

for $i=1, 2, 3, \cdots, \lambda-1$; $k=0, 1, 2, \cdots, \nu-1$, where

$$\nu = \frac{q^t - 1}{\lambda}.$$

We also have

$$(q^i - 1)(g^{i+\lambda} - 1)(g^{i+2\lambda} - 1) \cdots (g^{i+(\nu-1)\lambda} - 1) \equiv 1 - g^{\nu i} \pmod{\mathfrak{q}}$$

and

$$\sum \operatorname{ind}(g^{i+k\lambda} - 1) \equiv \operatorname{ind}(1 - g^{\nu i}) \equiv \operatorname{ind}(1 - \zeta_n^{\,i}) \pmod{l},$$

since $g^r \equiv \zeta_n \pmod{\mathfrak{q}}$. Carrying out the summation with respect to $k$, we have

$$\sum h^m \operatorname{ind}(g^h - 1) \equiv \sum_i i^m \operatorname{ind}(1 - \zeta_n^{\,i})$$

for $i=1, 2, 3, \cdots, \lambda-1$. Setting $i\gamma$ in place of $i$, multiplying by $\gamma^{-m}$ and subtracting the original from the second congruence, we have

$$(\gamma^{-m} - 1) \sum h^m \operatorname{ind}(g^h - 1) \equiv \sum i^m \operatorname{ind}\left(\frac{1 - \zeta_n^{\gamma i}}{1 - \zeta_n^{\,i}}\right).$$

Applying this to (8) we have an extension of (1).

THE UNIVERSITY OF TEXAS

# FERMAT'S LAST THEOREM AND THE SECOND FACTOR IN THE CYCLOTOMIC CLASS NUMBER

BY H. S. VANDIVER

1. *Introduction.* As usual in the relation

$$x^l + y^l + z^l = 0, \tag{1}$$

where $l$ is an odd prime and $x$, $y$, $z$ are rational integers prime to each other and none zero, we shall refer to the case where $xyz$ is prime to $l$ as case I; if $xyz \equiv 0 \pmod{l}$ then we call this case II. I now give a sketch of a proof of a theorem which appears to be the principal result I have so far found concerning the first case of the last theorem.

THEOREM 1. *If* (1) *is possible in case* I, *then the second factor of the class number of the cyclotomic field defined by*

$$\zeta = e^{2i\pi/l}$$

*is divisible by* $l$.

From (1) in case I we have either

$$x + \zeta y = \eta\omega_1\omega_2 \cdots \omega_s\alpha^l, \tag{2}$$

or

$$x + \zeta y = \sigma\beta^l, \tag{2a}$$

where $\eta$ and $\sigma$ are units, $\alpha$ is a number, and $\beta$ is an integer in $k(\zeta)$, while each $\omega$ is the $l$th power of an ideal in $k(\zeta)$, not a principal ideal, and, as shown by Pollaczek,*

$$\omega_i^{s-r\alpha_i} = \delta\gamma^l,$$

where $\delta$ is the unit in $k(\zeta)$, $a_i$ is in the set $1, 2, \cdots, l-2$, $r$ is a primitive root of $l$ and we are employing the Kronecker-Hilbert notation of symbolic powers, $s$ denoting the substitution $(\zeta/\zeta^r)$. We also have (Pollaczek†) for $a_i$ even

$$\omega_i/\omega_{-i} = \delta_i\gamma_i^l,$$

* Mathematische Zeitschrift, vol. 21 (1924), pp. 19 and 22.

† Loc. cit., p. 22.

where $\gamma_i$ is a number in $k(\zeta)$, $\delta_1$ is a unit and $\omega_{-i}$ is obtained from $\omega_i$ by the substitution $(\zeta/\zeta^{-1})$. Applying this to (2), we have

$$\frac{x+\zeta y}{x+\zeta^{-1}y} = \zeta^t \xi_1 \xi_2 \cdots \xi_s \theta^l, \tag{3}$$

where

$$\xi_i^{s-r^{2i+1}} = \eta_1 \theta_1^{\,l}, \tag{3a}$$

$\eta_1$ being a unit in $k(\zeta)$.

The writer* has shown that

$$\prod_{r=1}^{k-1} \prod_{a=1}^{[rl/k]} (x+\zeta^{[1:a]}y)^2 = \zeta^t \rho^{2l}, \tag{4}$$

where $k$ is an integer, $1<k<l$, $\rho$ is an integer in the field $k(\zeta)$, $t$ is an integer such that

$$t \equiv \frac{-2kyq(k)}{x+y} \pmod{l},$$

$[1:a]$ is the least positive solution of $Xa \equiv 1 \pmod{l}$, and $q(k)=(k^{l-1}-1)/l$. We also have

$$x+y=c^l, \tag{5}$$

where $c$ is a rational integer.

Let $\mathfrak{p}$ be a prime ideal divisor of one of the $\omega$'s in (2). In the relation (4) put $k=2$ and $\zeta^h$ for $\zeta$. We now employ this relation in much the same manner as in a former paper of the writer.† If in (4) there is an $a$ such that

$$h[1:a] \equiv 1 \pmod{l},$$

then set $\zeta^{-h}$ in lieu of $\zeta^h$ throughout the relation of (4). For $k=2$, $a$ ranges over the integers $1, 2, \cdots, (l-1)/2$. Then we cannot have any exponent of $\zeta$ which is $\equiv 1 \pmod{l}$, for if so we would have

$$-h[1:a_1] \equiv 1 \pmod{l},$$

where $a_1$ is one of the $a$'s. This gives

* Annals of Mathematics, vol. 26 (1925), p. 217.

† Annals of Mathematics, vol. 26 (1925), pp. 227–229.

$$[1:a_1] \equiv -[1:a] \pmod{l},$$

which is impossible.

Equating $l$th power characters of each member of (4) with respect to $\mathfrak{p}$ we obtain, since each binomial factor is prime to $x+\zeta y$,

$$\prod_a \left\{\frac{x+\zeta^{\pm h[1:a]}y}{\mathfrak{p}}\right\}^2 = \left\{\frac{\zeta^{\pm ht}}{\mathfrak{p}}\right\}; \tag{6}$$

when $k=2$ the sign of $h$ is selected so that

$$h[1:a] \not\equiv 1 \pmod{l}.$$

From the theorem of Furtwängler* we obtain

$$\left\{\frac{\zeta}{\mathfrak{p}}\right\} = 1.$$

Also we note that

$$x + \zeta^i y = (x+\zeta y) + y\zeta(\zeta^{i-1} - 1).$$

Applying this to (5), after taking $l$th power characters with respect to $\mathfrak{p}$, and also to (6), we have, after comparison,

$$\prod_a \left\{\frac{C_a}{\mathfrak{p}}\right\} = 1, \tag{7}$$

where

$$C_a = \frac{\zeta^{\pm h[1:a]-1} - 1}{\zeta - 1}.$$

Set

$$\sigma = \frac{\zeta^t - 1}{\zeta - 1},$$

where $t$ is any integer $\not\equiv 0 \pmod{l}$, and

$$\left\{\frac{\sigma}{\mathfrak{p}}\right\} = \zeta^T,$$

and write

* Wiener Berichte, Abteilung IIa, vol. 121 (1912), pp. 589–592.

$$T = \operatorname{ind}\left(\frac{\zeta^t - 1}{\zeta - 1}\right).$$

We then have (Vandiver*)

$$\operatorname{ind}\left(\frac{\zeta^t - 1}{\zeta - 1}\right) \equiv \frac{1}{2}(t-1)\operatorname{ind}\zeta - 2\sum_{n=1}^{l_1}\frac{(t^{2n}-1)\operatorname{ind}E_n(\zeta)}{r^{2n}-1} \pmod{l},$$

where

$$E_n = \prod_{i=0}^{l_1}\epsilon(\zeta^{r^i})^{r^{-2in}}, \quad \epsilon = \left(\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}\right)^{1/2}, \ (l_1 = l - 3/2).$$

Applying this to (7), we obtain

$$\sum_{n=1}^{l_1}\sum_{a=1}^{l_1+1}\frac{((\pm h[1:a]-1)^{2n}-1)\operatorname{ind}E_n(\zeta)}{r^{2n}-1} \equiv 0 \pmod{l}.$$

Now expanding the left hand members in powers of $h$, we find

$$\pm hA_1R_1 + h^2A_2R_2 + \cdots (\pm h)^{l-4}A_{l-4}R_{l-4} \equiv 0 \pmod{l},$$

where the $A$'s are expressions involving $r$ and $\operatorname{ind}E_n(\zeta)$, and

$$R_i = \sum_{a=1}^{l_1+1}[1:a]^i.$$

For $i$ even, this is known to be divisible by $l$ and we obtain

$$hA_1R_1 + h^3A_3R_3 + \cdots + h^{l-4}A_{l-4}R_{l-4} \equiv 0 \pmod{l}.$$

Letting $h = 1, 2, \cdots, l_1$ in turn, we obtain $l_1$ congruences and the determinant in the $AR$'s is an alternant which is prime to $l$, so that

$$A_jR_j \equiv 0 \pmod{l}, \qquad (j = 1, 3, \cdots, l-4).$$

We also have, if

$$b_1 = -\tfrac{1}{2}, \quad b_{2i} = (-1)^{i+1}B_i, \quad b_{2i+1} = 0, \qquad (i > 0),$$

where the $B$'s are Bernoulli's numbers,

* Transactions of this Society, vol. 31 (1929), p. 634.

$$\frac{(1-2^i)b_i}{2^{i-1}i} \equiv R_{l-i} \pmod{l}, \qquad (i < l-1);$$

$$(1-2^{2n})B_n A_{l-2n} \equiv 0 \pmod{l}, \qquad (n = 2, 3, \cdots, l_1).$$

Let $n = 2, 3, 4, 5, 6$, and 7. These give, except for small values of $l$ for which (1) is known to be impossible in case I, $A_{l-2n} \equiv 0 \pmod{l}$. We have

$$A_{l-4} = \frac{2(l-3)}{r^{l-3}-1} \operatorname{ind} E_{l_1}(\zeta);$$

hence

$$\operatorname{ind} E_{l_1}(\zeta) \equiv 0 \pmod{l}.$$

Similarly,

$$A_{l-6} = 2\binom{l-3}{3} \frac{\operatorname{ind} E_{l_1}(\zeta)}{r^{l-3}-1} + \frac{2(l-5)\operatorname{ind} E_{l_1-1}(\zeta)}{r^{l-5}-1},$$

which gives

$$\operatorname{ind} E_{l_1-1}(\zeta) \equiv 0 \pmod{l}.$$

Similarly,

$$\operatorname{ind} E_{l_1-j}(\zeta) \equiv 0 \pmod{l}, \qquad (j = 2, 3, 4, 5).$$

Now take any $(\omega)$ which appears in (2). There exists an ideal $\mathfrak{a}$, not principal, such that $\mathfrak{a}^{l^\sigma} = (\omega)$, but $\mathfrak{a}^{l^{\sigma-1}}$ is not principal. In lieu of $\mathfrak{p}$ in the above argument we may now set $\mathfrak{a}$ since it is the product of prime ideals. Then we may write

$$\left\{\frac{E_{l_1-j}(\zeta)}{\mathfrak{a}}\right\} = 1, \qquad (j = 0, 1, 2, 3, 4, 5).$$

We now have, however (Vandiver*), where $\operatorname{ind} E_n(\zeta)$ is taken with respect to $\mathfrak{a}$ in lieu of $\mathfrak{p}$,

$$\operatorname{ind} E_n \equiv \frac{r^{2n}-1}{2}(-1)^{(s-1)/2}\frac{B_{(s+1)/2}}{l^a} D(\omega', l) \pmod{l},$$

where

* Transactions of this Society, vol. 32 (1930), p. 400.

$$D(\omega', t) = \left[\frac{d^t \log \omega'(e^v)}{dv^t}\right]_{v=0},$$

$$t = (l - 2n)l^a, \quad \mathfrak{a}^{l^a(l-1)} = \omega', \quad \omega' \equiv 1 \pmod{\lambda},$$

$$\lambda = (1 - \zeta), \quad s = (2n - 1)l^a.$$

The second factor of the class number $k(\zeta)$ will now be assumed prime to $l$. We may employ a result in another paper (Vandiver*) and we see that $B_{(s+1)/2}$ is divisible by $l^a$, but not by $l^{a+1}$, so that $D(\omega', t) \equiv 0 \pmod{l}$, from which we obtain easily, provided $\mathfrak{a}$ belongs to the ideal class corresponding to $B_n$ in the sense of the theorem on page 206 of that paper,

$$\left[\frac{d^{l-2n} \log \omega(e^v)}{dv^{l-2n}}\right]_{v=0} \equiv 0 \pmod{l}. \tag{8}$$

From (3) and (3a) we may derive identities in $e^v$, and taking these in connection with (2) and (2a), we obtain

$$\left[\frac{d^k \log \xi_i(e^v)}{dv^k}\right]_{v=0} \equiv 0 \pmod{l}, \quad (l - 1 > k \not\equiv 2i + 1),$$

and also

$$\left[\frac{d^3 \log (x + e^v y)}{dv^3}\right]_{v=0} \equiv 0 \pmod{l},$$

after using (8) for $n = l_1$. In a similar way we obtain this relation with $(x, z)$ or $(y, z)$ in lieu of $(x, y)$. These relations will then give easily

$$x \equiv y \equiv z \pmod{l},$$

and this is impossible for $l > 3$. Hence the second factor of the class number is divisible by $l$. This completes the (abbreviated) proof of Theorem 1.

2. *Second Factor of $k(\zeta)$ Divisible by $l$.* The preceding methods yield some criteria also in the case where the second factor of the class number of $k(\zeta)$ is divisible by $l$. Using some results due to Pollaczek,† we shall find in this case that there exists a singu-

* Proceedings of the National Academy of Sciences, vol. 15 (1929), p. 206.

† Loc. cit., pp. 19–22.

lar primary unit in $k(\zeta)$ corresponding to certain $\omega$'s in (2). It may be shown from this that we must have some of the $E$'s equal to $l$th powers of units in $k(\zeta)$. In fact we find this result:*

THEOREM 2. *If the relation* (1) *is satisfied in case* I, *then, if* $\eta_j$ *is a unit in* $k(\zeta)$,

$$E_{l_1-j} = \eta_j^l, \qquad (j = 0, 1, 2, 3, 4, 5),$$

*and*

$$B_s \equiv 0 \pmod{l^2}, \quad (i = 1, 2, 3, 4, 5, 6; s = n_i(l_1 + 1) - i),$$

*where the n's each range independently over all positive integral values.*

Use of Theorems 1 and 2 enables us to extend theorems† which have already been found for case II of (1). For example, five theorems as mentioned in another paper can now all be given without restriction to case II only, which restriction appears in Theorems 1 and 4.

Elsewhere‡ the writer has shown that if (1) is satisfied with $y \equiv 0 \pmod{l}$, $xz \not\equiv 0 \pmod{l}$, $x+z \not\equiv 0 \pmod{n}$, with $n$ any integer $\not\equiv 0$ or $1 \pmod{l}$, then

$$q(n)D_0 \equiv 0, \quad q(n)B_{s+1}D_s \equiv 0 \pmod{l}, \quad (s = 1, 3, \cdots, l-4);$$

and in addition one of the following two relations holds:

$$q(n)D_{l-2} \equiv 0, \qquad q(n)\left(D_{l-2} + \frac{I(\zeta)}{2}\right) \equiv 0 \pmod{l},$$

where

$$q(n) = \frac{n^{l-1} - 1}{l}, \quad D_s = \sum_{d=1}^{l-1} d^s I(\zeta^d - \beta^a), \quad \left\{\frac{\zeta}{\mathfrak{p}}\right\} = \zeta^{I(\zeta)},$$

where $\beta$ is a primitive $(n-1)$th root of unity and $\mathfrak{p}$ is a prime ideal divisor of $n$.

---

* This result as far as the $B$'s are concerned is an extension of a theorem previously given by the writer, Proceedings of the National Academy of Sciences, vol. 16 (1930), p. 298.

† Vandiver, Proceedings of the National Academy of Sciences, vol. 17 (1931), pp. 670–671.

‡ Transactions of this Society, vol. 29 (1927), p. 161.

Now if in lieu of the assumption of $x+z\not\equiv 0 \pmod{n}$, which appeared in the above theorem, we have proved that $x+z\equiv 0 \pmod{n}$, we may proceed as in a former paper* and obtain the result that (1) is impossible if $y\equiv 0 \pmod{l}$, $xz\not\equiv 0 \pmod{l}$, and $x+z\equiv 0 \pmod{n}$, under the additional assumption that

$$\left\{\frac{E_a}{\mathfrak{p}}\right\} \neq 1$$

holds, where $a$ ranges over the values $a_1, a_2, \cdots, a_s$, these integers being the subscripts of the Bernoulli numbers in the set $B_1, B_2, \cdots, B_{l_1}$ which are divisible by $l$.

Putting the preceding results together, we obtain a new criterion for the impossibility of (1) if we note that case I of (1) is covered by our assumptions concerning $E_a$. We note also† that we may extend this to the case where

$$n \equiv 1 \pmod{l}.$$

The theorem last mentioned as well as Theorem 1 indicates that much of the writer's work concerning Fermat's Last Theorem is tending toward the possible conclusion that if the second factor of the class number of $k(\zeta)$ is prime to $l$, then Fermat's Last Theorem is true.

A curious point in connection with the second case of the theorem is the fact that it is not conclusive that any of the methods used so far absolutely depend on the fact that $x$, $y$, and $z$ in (1) are rational integers. For example, in Theorem V of a former article I employ the fact that $x$, $y$, and $z$ are rational integers during the proof, but it is not shown that a similar argument breaks down when $x$, $y$, and $z$ are integers‡ in the field $k(\zeta+\zeta^{-1})$.

In view of these considerations it may happen that Fermat's Last Theorem is true for rational integers, but for integers in the field of $k(\zeta+\zeta^{-1})$ it is not true. Possibly the method of infinite descent properly belongs to the treatment of this generalization.

---

* Transactions of this Society, vol. 31 (1929), p. 634.

† Transactions of this Society, vol. 29 (1927), p. 162, §5.

‡ Fueter raised this question in connection with Theorem 5, during a conversation with me.

A bit of light is shown on the possibilities mentioned in the last paragraph if we consider the argument employed to prove Theorem IV in another article.* In this proof we started with the relation $\omega^l+\theta^l+\phi^l=0$, where $\omega, \theta$, and $\phi$ are integers in the field $k(\zeta+\zeta^{-1})$. This assumption enabled us to transpose $\theta^l$ in the above relation, factor, and obtain the relation (25a) of the last mentioned paper. However, if we had started with the equation

$$\omega^l + \theta^l = \eta\phi^l,$$

where $\phi$ is divisible by $(1-\zeta)$, we would obtain, by proceeding somewhat as in the derivation of (25a) in the article just referred to,

$$\omega \equiv \pm\, \theta \pmod{\mathfrak{p}};$$

and if

$$\omega \equiv \theta \pmod{\mathfrak{p}},$$

then, using (1), we have

$$2\omega^l \equiv \eta\phi^l \pmod{\mathfrak{p}}.$$

This gives the result that $2/\eta$ is congruent to an $l$th power modulo $\mathfrak{p}$. It seems necessary then to include among our assumptions the statement that such a congruence does not hold, and this was not necessary in the case where $\eta=1$.

THE UNIVERSITY OF TEXAS

* Transactions of this Society, vol. 31 (1929), pp. 631–632.

# INDEPENDENT POSTULATES FOR THE "INFORMAL" PART OF PRINCIPIA MATHEMATICA*

BY E. V. HUNTINGTON

1. *Introduction.* It has long been recognized that Section A of Whitehead and Russell's *Principia Mathematica* contains two distinct theories of mathematical logic—one a "formal" or "official" theory, the other an "informal" or "unofficial" theory. The "formal" theory is embodied in a series of numbered propositions, while the "informal" theory includes, besides the numbered propositions, certain other propositions inserted by way of explanation or commentary. Since some of these explanatory propositions are actual additions to the text, not deducible from the numbered propositions, it appears that the "formal" theory is the more restricted (in the number of its theorems) and the "informal" theory the more inclusive of the two.

The contrast between these two theories presents an important problem in the foundations of mathematics; but in spite of the voluminous literature that has grown up around the "formal" theory during the last twenty years, little attention has been paid to the "informal" theory; moreover, the special notation in which the whole of the Principia is expressed is still unfamiliar to many mathematicians.

The purpose of the present paper is to show that the "informal" theory of the Principia, when translated into more familiar mathematical language, is capable of being represented by an ordinary abstract mathematical theory; and for this abstract mathematical theory a set of independent postulates is worked out in the usual way.†

---

* Presented to the Society, June 16, 1933.

† The scheme of translation here employed (representing the assertion sign by a "subclass $C$") was first used in 1933, in my paper entitled *New sets of independent postulates for the algebra of logic, with special reference to Whitehead and Russell's Principia Mathematica*, Transactions of this Society, vol. 35 (1933), pp. 274–304, with corrections on p. 557 and p. 971. The present paper is a simplification and extension of Appendix II of that paper. An earlier scheme of translation (representing the assertion sign by the notation "$=1$") is found in a paper by B. A. Bernstein entitled *Whitehead and Russell's theory of deduction as a mathematical science*, this Bulletin, vol. 37 (1931), pp. 480–488. The "sub-

2. *The Primitive Ideas* $(K, C, +, ')$. The primitive ideas in the abstract mathematical theory here proposed are four in number:

$K$ = an undefined class of elements, $a, b, c, \cdots$;

$C$ = an undefined subclass within the class $K$;

$a+b$ = the result of an undefined binary operation on $a$ and $b$;

$a'$ = the result of an undefined unary operation on $a$.

It will be assumed without further mention that the subclass $C$, and hence the main class $K$, is non-empty.

3. *The Postulates* P1–P8. The postulates which we propose to consider are the following eight.

POSTULATE P1. *If $a$ is in $K$ and $b$ is in $K$, then $a+b$ is in $K$.*

POSTULATE P2. *If $a$ is in $K$, then $a'$ is in $K$.*

(These two postulates merely ensure that the class $K$ is a "closed set" with respect to the operations $+$ and $'$.)

POSTULATE P3. *If $a$ is in $C$, then $a$ is in $K$.*

(This postulate merely ensures that $C$ is a subclass in $K$.)

In the following postulates, $a$ and $b$ are assumed to be elements of $K$.

POSTULATE P4. *If $a+b$ is in $C$, then $b+a$ is in $C$.*

POSTULATE P5. *If $a$ is in $C$, then $a+b$ is in $C$.*

DEFINITION. The notation ($a$ is in $C'$) shall mean ($a$ is in $K$ and $a$ is not in $C$).

POSTULATE P6. *If $a$ is in $K$ and $a'$ is in $C$, then $a$ is in $C'$.*

POSTULATE P7. *If $a$ is in $K$ and $a'$ is in $C'$, then $a$ is in $C$.*

POSTULATE P8. *If $a+b$ is in $C$ and $a'$ is in $C$, then $b$ is in $C$.*

Any system $(K, C, +, ')$ which satisfies these Postulates P1–P8 may be called an *informal Principia system*, for reasons which will be explained in a later section; and the independence of these eight postulates will be established in the usual way.

Three supplementary postulates, P9–P11, will be introduced in the following paper.

---

class $C$" is believed to be preferable to the "$=1$," since the notation "$=1$" appears to suggest that all true propositions are in some sense "equal" to a single (selected) proposition, whereas the "subclass $C$" does not suggest any such artificial restriction.

4. *Immediate Consequences of Postulates* P1–P8. The following theorems are immediate consequences of Postulates P1–P8, no matter what interpretation may be given to the undefined symbols ($K$, $C$, $+$, $'$).

P12. *If $a$ is in $C'$, then $a'$ is in $C$.*

PROOF. By definition, $a$ is in $K$ and $a$ is not in $C$. Hence by P2, $a'$ is in $K$. Suppose $a'$ is not in $C$. Then by definition, $a'$ is in $C'$, whence, by P7, $a$ is in $C$, contrary to hypothesis. Hence $a'$ is in $C$. (This Theorem P12 is the converse of P6.)

P13. *If $a$ is in $C$, then $a'$ is in $C'$.*

PROOF. By P3, $a$ is in $K$, whence by P2, $a'$ is in $K$. Suppose $a'$ is in $C$. Then by P6, $a$ is in $C'$, whence by definition, $a$ is not in $C$, contrary to hypothesis. Hence $a'$ is not in $C$. Hence by definition, $a'$ is in $C'$. (P13 is the converse of P7.)

P14. *If $a$ is in $K$ and $a$ is not in $C'$, then $a$ is in $C$.*

PROOF. Suppose $a$ is not in $C$. Then by definition and the first part of the hypothesis, $a$ is in $C'$, contrary to the second part of the hypothesis. Hence $a$ is in $C$.

COROLLARY 1. The class $K$ is divided into two non-empty, mutually exclusive subclasses, $C$ and $C'$, which together exhaust the class $K$. (Simple dichotomy.)

To prove that there exists at least one element in $C'$, note that, by tacit assumption, there exists at least one element $a$ in $C$; then this element $a$ determines an element $a'$ which by P13 is in $C'$. That $C$ and $C'$ are mutually exclusive and together exhaust the class $K$ follows from the definition of $C'$.

P15. *If $a+b$ is in $C'$, then $b+a$ is in $C'$.*

PROOF. By P1, $b+a$ is in $K$. Suppose $b+a$ is not in $C'$. Then by P14, $b+a$ is in $C$, whence by P4, $a+b$ is in $C$, contrary to hypothesis. Hence $b+a$ is in $C'$.

P16. *If $a+b$ is in $C$ and $a$ is in $C'$, then $b$ is in $C$.*

PROOF. By P12, $a'$ is in $C$. Hence, by P8, $b$ is in $C$.

COROLLARY 2. If $a+b$ is in $C$, then at least one of the elements $a$ and $b$ is in $C$.

P17. *If $a+b$ is in $C'$, then $a$ is in $C'$ and $b$ is in $C'$.*

PROOF. Suppose $a$ is not in $C'$. Then by P14, $a$ is in $C$, whence by P5, $a+b$ is in $C$, contrary to hypothesis. Hence $a$ is in $C'$. Again, suppose $b$ is not in $C'$. Then by P14, $b$ is in $C$, whence by P5, $b+a$ is in $C$, whence by P4, $a+b$ is in $C$, contrary to hypothesis. Hence $b$ is in $C'$.

P18. *If $a$ is in $C'$ and $b$ is in $C'$, then $a+b$ is in $C'$.*

PROOF. Suppose $a+b$ is not in $C'$. Then by P14, $a+b$ is in $C$, whence by P16 and the first part of hypothesis, $b$ is in $C$, contrary to the second part of hypothesis. Hence $a+b$ is in $C'$.

P19. (1) *If $a$ is in $C$, then $(a')'$ is in $C$; and conversely.*
(2) *If $(a')'$ is in $C$, then $a$ is in $C$.*
(3) *If $a$ is in $C'$, then $(a')'$ is in $C'$; and conversely.*
(4) *If $(a')'$ is in $C'$, then $a$ is in $C'$.*

PROOF. (1) By P13, $a'$ is in $C'$, whence by P12, $a''$ is in $C$.
(2) By P6, $a'$ is in $C'$, whence by P7, $a$ is in $C$.
(3) By P12, $a'$ is in $C$, whence by P13, $a''$ is in $C'$.
(4) By P7, $a'$ is in $C$, whence by P6, $a$ is in $C'$.

5. *Deduction of* P20–P29 *from* P1–P8. The following theorems P20–P29 are further consequences of Postulates P1–P8. (The references in brackets are to the Principia, as explained in the following section.)

P20. *If $a$ is in $C$, then $a$ is in $K$.* [Page 92(3)]
P21. *If $a$ is in $C$ and $a'+b$ is in $C$, then $b$ is in $C$.* [*1.1]
P22. *If $a$ is in $K$, then $(a+a)'+a$ is in $C$.* [*1.2]
P23. *If $a, b$, etc. are in $K$, then $b'+(a+b)$ is in $C$.* [*1.3]
P24. *If $a, b$, etc. are in $K$, then $(a+b)'+(b+a)$ is in $C$.* [*1.4]
P25. *If $a, b, c$, etc. are in $K$, then $(b'+c)'+[(a+b)'+(a+c)]$ is in $C$.* [*1.6]
P26. *If $a$ is in $K$ and $b$ is in $K$, then $a+b$ is in $K$.* [*1.71]
P27. *If $a$ is in $K$, then $a'$ is in $K$.* [*1.7]
P28. *If $a'$ is in $C$, then $a$ is not in $C$.* [Page 93(5)]
P29. *If $a+b$ is in $C$, then at least one of the elements $a$ and $b$ is in $C$.* [Page 93(6)]

Of these theorems, P20, P26, P27, P28, P29 follow at once from P3, P1, P2, P6, P16. The proofs of the remaining theorems are as follows.*

* For valuable suggestions in this connection I am indebted to Alonzo Church and K. E. Rosinger.

PROOF OF P21. From $a$ in $C$ follows $a''$ in $C$ (by P13 and P12). Hence we have $a''$ in $C$ and $a'+b$ in $C$, whence by P8, $b$ is in $C$.

PROOF OF P22. If $a$ is in $C$, then by P5 and P4, $(a+a)'+a$ is in $C$. If $a$ is not in $C$, then $a$ is in $C'$, whence by P18, $a+a$ is in $C'$, whence by P12, $(a+a)'$ is in $C$, whence by P5, $(a+a)'+a$ is in $C$.

PROOF OF P23. If $b$ is in $C$, then by P5 and P4, $a+b$ is in $C$, whence by P5 and P4, $b'+(a+b)$ is in $C$. If $b$ is not in $C$, then $b$ is in $C'$, whence by P12, $b'$ is in $C$, whence by P5, $b'+(a+b)$ is in $C$.

PROOF OF P24. Suppose $(a+b)'+(b+a)$ is not in $C$. Then $(a+b)'+(b+a)$ is in $C'$, whence by P17, $(a+b)'$ is in $C'$, whence by P7, $a+b$ is in $C$, whence by P4, $b+a$ is in $C$, whence by P5 and P4, $(a+b)'+(b+a)$ is in $C$.

PROOF OF P25. Suppose $(b'+c)'+[(a+b)'+(a+c)]$ is in $C'$. Then by P17, $(a+b)'+(a+c)$ is in $C'$, whence by P17, $a+c$ is in $C'$, whence by P17, $a$ is in $C'$ and $c$ is in $C'$. By P12, $a'$ is in $C$. Also, by P17, $(a+b)'$ is in $C'$, whence by P7, $a+b$ is in $C$, whence by P8, $b$ is in $C$, whence by P13, $b'$ is in $C'$. Then by P18, $b'+c$ is in $C'$, whence by P12, $(b'+c)'$ is in $C$, whence by P5, $(b'+c)'+[(a+b)'+(a+c)]$ is in $C$.

6. *Correspondence between* P20–P29 *and the "Informal" Principia.* The validity of Theorems P20–29 of course does not depend on any particular interpretation of the undefined symbols ($K$, $C$, $\vdash$, $'$). But if the undefined class $K$ is interpreted as the class of entities called "elementary propositions" in the Principia; and if the undefined subclass $C$ is interpreted as the class of "true" elementary propositions, distinguished from other propositions in the Principia by the use of the assertion sign, $\vdash$; and if the undefined element $a+b$ is interpreted as the proposition "$a$ or $b$," denoted in the Principia by $a \vee b$ (conveniently read "$a$ wedge $b$"); and if the undefined element $a'$ is interpreted as the proposition "not-$a$," denoted in the Principia by $\sim a$ (conveniently read "curl $a$"); then these propositions P20–P29 will be found to correspond precisely to the "primitive propositions" on which the "informal" theory of the Principia is based.*

* The words "wedge" and "curl" (like the word "horse-shoe") are due to H. M. Sheffer.

Thus, Theorem P20 corresponds to the fact that in the Principia a "true proposition" is at any rate a "proposition"; Theorems P21–P27 correspond to the "formal" primitive propositions in the Principia, as indicated by the starred numbers in brackets; Theorem P28 corresponds to the Principia's "informal" explanation of the meaning of $\sim a$; and Theorem P29 corresponds to the Principia's "informal" explanation of the meaning of $a \vee b$.

Hence our deduction of Theorems P20–P29 from the Postulates P1–P8 is in effect a deduction of the whole "informal" system of the Principia from these Postulates P1–P8.*

7. *Deduction of* P1–P8 *from* P20–P29. We now show, conversely, that P1–P8 can be deduced from P20–P29, no matter

---

* In detail, the steps of the translation may be justified as follows.

The translation of the assertion sign, "$\vdash$," into the "subclass $C$" is suggested by the following statement on page 92 of the Principia (vol. I, second edition, 1925): "The sign '$\vdash$' may be read 'it is true that';" thus "$\vdash:\sim p \vee q$" means "it is true that either $p$ is false or $q$ is true."

The theorems P28 and P29 are translations of the following passages on page 93 of the Principia: "The proposition '$\sim p$' means 'not-$p$' or '$p$ is false';" and "The proposition '$p \vee q$' means 'either $p$ is true or $q$ is true,' where the alternatives are not to be mutually exclusive."

The translation of *1.2, *1.3, *1.4, *1.6 into P22–P25 is immediate, in view of the definition of $p \supset q$ in *1.01, namely, $p \supset q \cdot = \cdot \sim p \vee q$.

The translation of *1.71 and *1.7 into P26 and P27 is also immediate.

In regard to *1.1, which reads in the original: "Anything implied by a true elementary proposition is true," the authors of the Principia state that they "cannot express this principle symbolically," and that it is not the same as "if $p$ is true, then if $p$ implies $q$, $q$ is true." But in view of the Principia's definition of "$p$ implies $q$," namely, $\sim p \vee q$ (*1.01), and in view of the actual use which is made of *1.1 throughout the Principia (in which connection *8.12 is of interest), it appears that for our present purposes *1.1 may fairly be translated into P21.

The primitive proposition *1.5 (the associative law for $\vee$) is omitted because it is now known to be a consequence of the other numbered primitive propositions (proof by Bernays in 1926, reproduced in Transactions of this Society, vol. 35 (1933), p. 292).

The primitive propositions *1.11 and *1.72, together with the primitive idea "assertion of a propositional function," are omitted in accordance with instructions found in the Introduction to the second edition of the Principia, page xiii.

Thus all the primitive ideas and primitive propositions of the "informal" Principia are accounted for.

what interpretation may be given to the undefined symbols $(K, C, +, ')$.

P1, P2, P3.

These propositions follow immediately from P26, P27, P20.

P4. If $a+b$ is in $C$, then $b+a$ is in $C$.

PROOF. By hypothesis, $a+b$ is in $C$. By P24, $(a+b)'+(b+a)$ is in $C$. Hence by P21, $b+a$ is in $C$.

P5. If $a$ is in $C$, then $a+b$ is in $C$.

PROOF. By P23, $a'+(b+a)$ is in $C$. Hence by P21, $b+a$ is in $C$, whence by P4, $a+b$ is in $C$.

DEFINITION. ($a$ is in $C'$) means ($a$ is in $K$ and $a$ is not in $C$).

LEMMA. If $a$ is in $K$, then $a'+a$ is in $C$.

PROOF. Case 1. Suppose $a'$ is in $C$. Then by P5, $a'+a$ is in $C$. Case 2. Suppose $a'$ is not in $C$. By P23, $a'+(a'+a)$ is in $C$. Hence by P29, $a'+a$ is in $C$.

ALTERNATIVE PROOF (without using P29). By P25, $[(a+a)'+a]'+\{[a'+(a+a)]'+(a'+a)\}$ is in $C$. But by P22, $(a+a)'+a$ is in $C$. Hence by P21, $[a'+(a+a)]'+(a'+a)$ is in $C$. But by P23, $a'+(a+a)$ is in $C$. Hence by P21, $a'+a$ is in $C$.

P6. If $a$ is in $K$ and $a'$ is in $C$, then $a$ is in $C'$.

PROOF. By P28 and the definition of $C'$.

P7. If $a$ is in $K$ and $a'$ is in $C'$, then $a$ is in $C$.

PROOF. By lemma, $a'+a$ is in $C$. But by definition, $a'$ is not in $C$. Hence by P29, $a$ is in $C$.

P8. If $a+b$ is in $C$ and $a'$ is in $C$, then $b$ is in $C$.

PROOF. By P28, $a$ is not in $C$. Hence by P29, $b$ is in $C$.

We note in passing that P22 and P25 are deducible from the other propositions of the list P20–P29.

8. *Equivalence of the "Informal" Principia and Postulates* P1–P8. The propositions P20–P29 have been deduced from P1–P8; and conversely, P1–P8 have been deduced from P20–P29; so that the set of propositions P1–P8 is equivalent to the set of propositions P20–P29. But P20–P29 have been shown to correspond to the primitive propositions of the "informal" Principia. Hence, if our scheme of translation is adequate, the Postulates P1–P8 fairly represent the whole "informal" theory of the Principia.

9. *Independence of Postulates* P1–P8. The independence of Postulates P1–P8 is established by the following examples of systems $(K, C, +, ')$, each of which violates the like-numbered postulate and satisfies all the others.

EXAMPLE P1.

$K$ = a class of four elements, represented by the "tags" 1, 2, 3, 4;
$C = 1, 2$;
$a+b$ and $a'$ as in the table ($w$ being any number not in the class $K$).
Here P1 clearly fails. All the other postulates are satisfied.

| $+$ | 1 | 2 | 3 | 4 | $'$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 4 |
| 2 | 1 | 2 | 1 | 2 | 3 |
| 3 | 1 | 1 | 3 | $w$ | 2 |
| 4 | 1 | 2 | $w$ | 4 | 1 |

EXAMPLE P2.

$K = 1, 2, 3, 4$;
$C = 1, 2$;
$a+b$ and $a'$ as in the table.
Here P2 fails since $1'$ is not in $K$.
All the other postulates are satisfied.

| $+$ | 1 | 2 | 3 | 4 | $'$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | $w$ |
| 2 | 1 | 2 | 1 | 2 | 3 |
| 3 | 1 | 1 | 3 | 3 | 2 |
| 4 | 1 | 2 | 3 | 4 | 1 |

EXAMPLE P3.

$K = 1, 2$;
$C = 1, 3$;
$a+b$ and $a'$ as in the table.
Here P3 fails on $a = 3$.
All the other postulates are found to be satisfied (the subclass $C'$ comprising the single element 2).

| $+$ | 1 | 2 | 3 | $'$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 2 |
| 2 | 1 | 2 | $w$ | 1 |
| 3 | 1 | $w$ | 3 | 3 |

EXAMPLE P4.

$K = 1, 2, 3, 4$;
$C = 1, 2$;
$a+b$ and $a'$ as in the table.
Here P4 fails, since $1+3(=1)$ is in $C$ and $3+1\ (=3)$ is not. The other seven postulates are all satisfied. (Postulate P8 is satisfied "vacuously," since the condition $a+b$ in $C$ and $a'$ in $C$ does not occur in this system.) Note. This system does not satisfy the commutative law $a+b=b+a$.

| $+$ | 1 | 2 | 3 | 4 | $'$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 4 |
| 2 | 2 | 2 | 2 | 2 | 3 |
| 3 | 3 | 3 | 3 | 3 | 2 |
| 4 | 4 | 4 | 4 | 4 | 1 |

EXAMPLE P5.

$K = 1, 2, 3, 4$;
$C = 1, 2$;
$a+b$ and $a'$ as in the table
Here P5 fails, since 2 is in $C$ and $2+3$ is not. All the other postulates are found to satisfied (P8 vacuously).

| $+$ | 1 | 2 | 3 | 4 | $'$ |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 4 |
| 2 | 2 | 2 | 4 | 4 | 3 |
| 3 | 3 | 4 | 3 | 4 | 2 |
| 4 | 4 | 4 | 4 | 4 | 1 |

EXAMPLE P6.

$K = 1, 2, 3, 4$;
$C = 1, 2, 3, 4$;
$a+b$ and $a'$ as in the table. Here $C'$ is empty.
Postulate P6 fails, since $2'$ $(=3)$ is in $C$ and 2 is not in $C'$. All the other postulates are satisfied (P7 vacuously).

| $+$ | 1 | 2 | 3 | 4 | $'$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 4 |
| 2 | 1 | 2 | 1 | 2 | 3 |
| 3 | 1 | 1 | 3 | 3 | 2 |
| 4 | 1 | 2 | 3 | 4 | 1 |

EXAMPLE P7.

$K = 1, 2, 3, 4$;
$C = 1$;
$a+b$ and $a'$ the same as in the table for Example P6. Here $C' = 2, 3, 4$. Postulate P7 fails, since $2'$ $(=3)$ is in $C'$ and 2 is not in $C$. All the other postulates are satisfied.

EXAMPLE P8.

$K = 1, 2, 3, 4, 5, 6, 7, 8$;
$C = 1, 2, 3, 4$;
$a+b$ and $a'$ as in the table.
Here P8 fails, since $5+6$ is in $C$ and $5'$ is in $C$ but 6 is not in $C$. All the other postulates are satisfied.

| $+$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | $'$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 2 | 1 | 2 | 1 | 1 | 2 | 2 | 1 | 2 | 7 |
| 3 | 1 | 1 | 3 | 1 | 3 | 1 | 3 | 3 | 6 |
| 4 | 1 | 1 | 1 | 4 | 1 | 4 | 4 | 4 | 5 |
| 5 | 1 | 2 | 3 | 1 | 5 | 2 | 3 | 5 | 4 |
| 6 | 1 | 2 | 1 | 4 | 2 | 6 | 4 | 6 | 3 |
| 7 | 1 | 1 | 3 | 4 | 3 | 4 | 7 | 7 | 2 |
| 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 |

These eight examples show that no one of the Postulates P1–P8 can be deduced from the other seven.

10. *Examples of Systems* $(K, C, +, ')$ *Satisfying Postulates* P1–P8. The *consistency* of the Postulates P1–P8 is established

by the existence of any one of the following examples of systems $(K, C, +, ')$, each of which satisfies all the postulates.

EXAMPLE 0.1.

$K$ = the class comprising the two numbers 1 and 2;

$C$ = the class comprising the single number 1;

$a+b$ and $a'$ = the numbers given by the adjoining table.

| $+$ | 1 | 2 | $'$ |
|---|---|---|---|
| 1 | 1 | 1 | 2 |
| 2 | 1 | 2 | 1 |

EXAMPLE 0.2.

$K$ = the four numbers 1, 2, 3, 4;

$C$ = the two numbers 1, 2;

$a+b$ and $a'$ = the numbers given by the table.

| $+$ | 1 | 2 | 3 | 4 | $'$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 4 |
| 2 | 1 | 2 | 1 | 2 | 3 |
| 3 | 1 | 1 | 3 | 3 | 2 |
| 4 | 1 | 2 | 3 | 4 | 1 |

EXAMPLE 0.3.

$K$ = 1, 2, 3, 4, 5, 6, 7, 8;

$C$ = 1, 2, 3, 4;

$a+b$ and $a'$ as given by the table.

| $+$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | $'$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 7 |
| 3 | 1 | 1 | 3 | 3 | 1 | 1 | 3 | 3 | 6 |
| 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 |
| 5 | 1 | 1 | 1 | 1 | 5 | 5 | 5 | 5 | 4 |
| 6 | 1 | 2 | 1 | 2 | 5 | 6 | 5 | 6 | 3 |
| 7 | 1 | 1 | 3 | 3 | 5 | 5 | 7 | 7 | 2 |
| 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 |

Other examples will be found in the following supplementary paper.

HARVARD UNIVERSITY

# INDEPENDENT POSTULATES FOR AN "INFORMAL PRINCIPIA SYSTEM WITH EQUALITY"*

BY E. V. HUNTINGTON

1. *Introduction.* The Postulates P1–P8 in the preceding paper define an abstract mathematical system $(K, C, +, ')$ which has there been called an "informal Principia system."

An interesting concrete illustration of this abstract mathematical theory may be developed as follows.

2. *A System of "Verdicts" and the Idea of Equality.* Consider a group of people, $A, B, C, \cdots$, each of whom is supposed to be either "guilty" or "not guilty" on some charge before a court. A judgment of the court such as "$A$ is guilty" or "$B$ is not guilty" may be called a "simple verdict," while any combination of two or more such simple verdicts by means of the connectives "or" and "and" may be called a "compound verdict." For example, the statement "$A$-is-guilty-and-$B$-is-not-guilty or $C$-is-guilty" is a compound verdict. (The word "or" is to be understood in the sense of "at least one.")

Clearly, if $a$ is a verdict and $b$ is a verdict, then the statement "$a$ and $b$" is a verdict, and also the statement "$a$ or $b$" is a verdict.

To every verdict, $a$, there corresponds a "contradictory" verdict, which we shall denote by $-a$. If $a$ is a verdict, then the "contradictory of $a$" is to be understood in the usual linguistic sense. For example:

if $a =$ "$A$ is guilty," then $-a =$ "$A$ is not guilty";
if $a =$ "$A$ is not guilty," then $-a =$ "$A$ is guilty";
if $a =$ "$A$ is guilty and $B$ is not guilty," then
$-a =$ "$A$ is not guilty or $B$ is guilty";
if $a =$ "$A$ is guilty or $B$ is not guilty," then
$-a =$ "$A$ is not guilty and $B$ is guilty";
if $a =$ "$A$-is-guilty-and-$B$-is-not-guilty or $C$ is-guilty," then
$-a =$ "$A$-is-not-guilty-or-$B$-is-guilty and $C$-is-not-guilty"; etc.

Clearly, if $a$ is any verdict, than $-a$ is also a verdict.

---

* Presented to the Society, December 27, 1933.

Further, every verdict is supposed to be either "correct" or "incorrect" under the law.

It must be noted, however, that if $a$ is a verdict, then the statement "$a$ is correct" is not itself a verdict; and similarly, if $a$ is a verdict, then the statement "$a$ is incorrect" is not itself a verdict. In other words, the attributes "guilty" and "not guilty" apply only to the people, $A, B, C, \cdots$, while the attributes "correct" and "incorrect" apply only to the verdicts of the court.

Further, we observe that among the "correct" verdicts there are some which are "necessarily correct," irrespective of the law in the case. For example, if $a =$"$A$ is guilty or $A$ is not guilty," then $a$ is a necessarily correct verdict. Such verdicts we may call "truistic verdicts," or simply "truisms."

Similarly, among the "incorrect" verdicts there are some which are "necessarily incorrect." For example, the verdict "$A$ is guilty and $A$ is not guilty" is a necessarily incorrect verdict. Such verdicts we may call "absurd verdicts" or simply "absurdities."

Finally, verdicts may be classified according to the effects which they produce on the personal fate of the individual defendents $A, B, C, \cdots$. For example, the verdict "$A$ is guilty" will send Mr. $A$ to jail, while the verdict "$B$ is not guilty" will free Mr. $B$ from the charge against him. The verdict "$A$ is guilty or $B$ is guilty," though it does not directly send anybody to jail, does affect the legal status of both $A$ and $B$; for if this verdict is followed later by the verdict "$B$ is not guilty," the result will be to send $A$ to jail. On the other hand, a truistic verdict, like "$A$ is guilty or $A$ is not guilty," or an absurd verdict, like "$A$ is guilty and $A$ is not guilty," will have no effect on anybody's fate.

If two correct verdicts, $a$ and $b$, are "equal" with respect to legal effect—that is, if $a$ and $b$ can be interchanged in the history of the decisions of the court without affecting, directly or ultimately, the legal fate of any person in the group considered —then we write "$a = b$." Similarly, if two incorrect verdicts, $a$ and $b$, are equal with respect to legal effect, then also we write "$a = b$."

For example, suppose $a$ means "$A$ is guilty" and $b$ means "$A$-is-guilty-and-$B$-is-guilty or $A$-is-guilty-and-$B$-is-not-guilty,"

then $a=b$; for the legal effect of the two verdicts is precisely the same, namely, to send $A$ to jail and to do nothing to $B$ or to any other defendant. Again, any truistic verdict will be "equal" to any other truistic verdict, and any absurd verdict will be "equal" to any other absurd verdict; but no correct verdict will be "equal" to any incorrect verdict. It need hardly be said that the notation "$a=b$" does not mean that $a$ and $b$ are "identical in all respects," which is an indefensible concept; here, as elsewhere in mathematics, $a=b$ means merely that $a$ and $b$ are identical in some respect, which must be specified.

The idea of equality does not occur in the primitive propositions of the Principia, and hence the equality sign is not used in our Postulates P1–P8. In the next section we propose to extend the abstract theory of systems $(K, C, +, ')$ so as to include systems, $(K, C, +, ')$ making use of the idea of equality. Such systems for lack of a better notation, we shall indicate by $(K, C, +, ', =)$, although the role of the "$=$" sign is clearly not quite analogous to the role of the other variables.* That is, "$=$" is not a wholly undefined relation; $a=b$ indicates merely that $a$ and $b$ are equal in some undefined respect, it being understood that if $a$ and $b$ are "equal" in this respect, either one may be replaced by the other wherever it occurs within the system $(K, C, +, ', =)$.

3. *Systems* $(K, C, +, ', =)$. *Postulates* P1–P11. Let us consider an abstract system $(K, C, +, ', =)$, where

$K$ = an undefined class of elements, $a, b, c, \cdots$;

$C$ = an undefined subclass within $K$ assumed non-empty;

$a+b$ = the result of an undefined binary operation on $a$ and $b$;

$a'$ = the result of an undefined unary operation on $a$; and

$a=b$ means $a$ and $b$ are equal in some undefined respect (see above);

and let us impose the following postulates, P1–P11:

POSTULATE P1. *If $a$ is in $K$ and $b$ is in $K$, then $a+b$ is in $K$.*

POSTULATE P2. *If $a$ is in $K$, then $a'$ is in $K$.*

POSTULATE P3. *If $a$ is in $C$, then $a$ is in $K$.*

POSTULATE P4. *If $a+b$ is in $C$, then $b+a$ is in $C$.*

POSTULATE P5. *If $a$ is in $C$, then $a+b$ is in $C$.*

* Compare K. Yoneyama, in the Tôhoku Mathematical Journal, vol. 22 (1923), p. 101, and vol. 24 (1925), pp. 287–293.

DEFINITION. The notation ($a$ is in $C'$) means ($a$ is in $K$ and $a$ is not in $C$).

POSTULATE P6. *If $a$ is in $K$ and $a'$ is in $C$, then $a$ is in $C'$.*

POSTULATE P7. *If $a$ is in $K$ and $a'$ is in $C'$, then $a$ is in $C$.*

POSTULATE P8. *If $a+b$ is in $C$ and $a'$ is in $C$, then $b$ is in $C$.*

In the following postulates, $a$, $b$, $a+b$, $a'$, $b'$, etc., are understood to be elements of $K$.

POSTULATE P9. $a+b=b+a$.

POSTULATE P10. $(a+b)+c=a+(b+c)$.

POSTULATE P11. $(a'+b')'+(a'+b)'=a$.

[If we introduce the usual definition of $ab$, namely,

DEFINITION. $ab=(a'+b')'$,

then Postulate P11 may be replaced by the following:

POSTULATE P11a. $ab+ab'=a$.]

Now any system ($K$, $C$, $+$, $'$) which satisfies Postulates P1–P8 has just been called an "informal Principia system." Hence any system ($K$, $C$, $+$, $'$, $=$) which satisfies Postulates P1–P11 may be called an "*informal Principia system with equality.*"

On the other hand, any system ($K$, $+$, $'$, $=$) which satisfies the five postulates P1, P2, P9, P10, P11 is known to be a Boolean algebra.* Hence any system ($K$, $C$, $+$, $'$, $=$) which satisfies Postulates P1–P11 may be called a "*Boolean algebra with subclass $C$.*"

This result, that an "informal Principia system with equality" is the same thing as a "Boolean algebra with subclass $C$," has an immediate bearing on the much-discussed problem of the proper relation between the "algebra of propositions" and the "algebra of classes."

4. *On the Independence of Postulates* P1–P11. In regard to the independence of Postulates P1–P11, it is obvious that Postulate P4 becomes redundant as soon as P9 is added. With the exception of Postulate P4, all the postulates are independent.

To prove this, we notice first that all the Examples P1–P8 above (with the added specification that "$=$" shall mean "equal with respect to numerical value") are found to satisfy Postulates P9–P11, except that Example P4 does not satisfy Postulate P9. Hence Postulates P1–P3, P5–P8 remain independent even after

* See my *fourth set* of postulates for Boolean algebra, Transactions of this Society, vol. 35 (1933), p. 280 and p. 557; or Mind, vol. 42 (1933), pp. 203–207.

P9–P11 have been added. The following supplementary examples prove the independence of P9–P11.

EXAMPLE P9.
$K=1, 2, 3, 4, 5, 6$;
$C=1, 2, 3$;
$a+b$ and $a'$ as in the table;
"$=$" means equal in numerical value. Here P9 fails, since $4+5=4$ and $5+4=5$. All the other postulates (including P4) are satisfied.

| $+$ | 1 | 2 | 3 | 4 | 5 | 6 | $'$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 6 |
| 2 | 1 | 2 | 2 | 1 | 1 | 2 | 5 |
| 3 | 1 | 3 | 3 | 1 | 1 | 3 | 4 |
| 4 | 1 | 1 | 1 | 4 | 4 | 4 | 3 |
| 5 | 1 | 1 | 1 | 5 | 5 | 5 | 2 |
| 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 |

EXAMPLE P10.
$K=1, 2, 3, 4, 5, 6, 7, 8$;
$C=1, 2, 3, 4$;
$a+b$ and $a'$ as in the table;
"$=$" means equal in numerical value.
Here P10 fails, since $(2+5)+7\neq 2+(5+7)$. All the other postulates are satisfied.

| $+$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | $'$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 |
| 2 | 1 | 2 | 3 | 4 | 3 | 4 | 1 | 2 | 7 |
| 3 | 1 | 3 | 3 | 1 | 3 | 1 | 1 | 3 | 6 |
| 4 | 1 | 4 | 1 | 4 | 1 | 4 | 2 | 4 | 5 |
| 5 | 1 | 3 | 3 | 1 | 5 | 7 | 5 | 5 | 4 |
| 6 | 1 | 4 | 1 | 4 | 7 | 6 | 7 | 6 | 3 |
| 7 | 1 | 1 | 1 | 2 | 5 | 7 | 7 | 7 | 2 |
| 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 |

EXAMPLE P11.
$K=1, 2, 3, 4$;
$C=1, 2$;
$a+b$ and $a'$ as in the table;
"$=$" means equal in numerical value.
Here P11 fails when $a=1$, $b=2$. All the other postulates are satisfied.

| $+$ | 1 | 2 | 3 | 4 | $'$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 4 |
| 2 | 1 | 2 | 2 | 2 | 3 |
| 3 | 1 | 2 | 3 | 3 | 2 |
| 4 | 1 | 2 | 3 | 4 | 1 |

We have thus established the fact that no one of the eleven postulates P1–P11 can be deduced from the other ten (except that P4 is a consequence of P9).

5. *Examples of Systems* $(K, C, +, ', =)$ *which Satisfy all the Postulates.* The Examples 0.1, 0.2, and 0.3, given on page 136, will be found to satisfy all the postulates P1–P11, when "$=$" is understood to mean "equal with respect to numerical value." More interesting examples are the following.

EXAMPLE 0.4.

$K$ = the class of "verdicts," $a, b, c, \cdots$, as explained above.

$C$ = the subclass of verdicts which are "correct";

$a+b$ = the statement "$a$ or $b$";

$a'$ = the statement contradictory to $a$;

$a=b$ means that $a$ and $b$ are "equal with respect to legal effect."

Here all the postulates are found to be satisfied. The subclass $C'$ comprises the "incorrect" verdicts, and $ab$ = the statement "$a$ and $b$." The "truistic" verdicts are all equal to the "universe element," $U$, of the Boolean algebra.

EXAMPLE 0.5.

$K$ = the class of "verdicts," $a, b, c, \cdots$, as above:

$C$ = the subclass of verdicts which are "incorrect";

$a+b$ = the statement "$a$ and $b$";

$a'$ = the statement contradictory to $a$;

$a=b$ means that $a$ and $b$ are "equal with respect to legal effect."

Here again all the postulates are found to be satisfied. The subclass $C'$ comprises the "correct" verdicts, and $ab$ = the statement "$a$ or $b$." The "truistic" verdicts are all equal to the "zero element," $Z$, of the Boolean algebra.

These last two examples illustrate the "principle of duality" between $+$ and $\times$. In Example 0.4, $+$ = "or," $\times$ = "and," and $C$ = "correct." In Example 0.5, $+$ = "and," $\times$ = "or," and $C$ = "incorrect."

The existence of any one of these five examples establishes the "consistency" of Postulates P1–P11.

Any one of these five systems is an example of an "informal Principia system with equality" (or a "Boolean algebra with subclass $C$").*

HARVARD UNIVERSITY

* *Note on the "formal" theory of the Principia.* Any system $(K, C, +, ', =)$ which satisfies all the postulates P1–P11 except P7, and violates P7, may be called a "*formal Principia system with equality.*"

For, it can easily be shown that from the Postulates P1–P11 without P7 we can deduce all the "formal" propositions P20–P28, but not the "informal" proposition P29. And conversely, from the "formal" propositions P20–P28, taken in conjunction with the propositions about equality, P9–P11, we can deduce all the Postulates P1–P6, P8–P11, but not P7. (Here, for the moment,

# A CYCLIC INVOLUTION OF ORDER SEVEN

BY W. R. HUTCHERSON

1. *Introduction.* In an earlier paper,† the writer discussed a cubic surface in ordinary three way space containing an involution of order five, $I_5$. This paper concerns itself with a different cubic surface which contains a cyclic involution, $I_7$.

2. *Discussion of $I_7$ Belonging to $F_3$ in $S_3$.* Consider the surface

$$F_3(x_1,x_2,x_3,x_4) \equiv ax_2^2x_3 + bx_3^2x_1 + cx_1x_2x_4 = 0$$

in $S_3$, invariant under the cyclic collineation $T$ of order seven

$$x_1' : x_2' : x_3' : x_4' = x_1 : \epsilon x_2 : \epsilon^2 x_3 : \epsilon^3 x_4, \qquad (\epsilon^7 = 1).$$

There are four invariant points, $P_1 \equiv (1, 0, 0, 0)$, $P_2 \equiv (0, 1, 0, 0)$, $P_3 \equiv (0, 0, 1, 0)$, and $P_4 \equiv (0, 0, 0, 1)$. Each lies on the surface $F$, and since these are the only possible invariant points, the surface $F$ has only four points of coincidence. It will be noticed, however, that only $P_2$ and $P_3$ are simple points of $F$. Hence this paper will not be interested in the two double invariant points, $P_1$ and $P_4$.

Consider a curve $C$, not transformed into itself by $T$, and passing through $P_2$. Take the plane $x_3+\lambda x_4=0$ of the pencil passing through $P_2$ and $P_1$, tangent to $C$. This plane is transformed into

---

P28 and its equivalent P6 are regarded as part of the "formal" theory; but both may be omitted, if preferred, without prejudice to the other postulates.)

What is perhaps the most obvious example of a "formal Principia system with equality" is the system ($K$, $C$, $+$, $'$, $=$) obtained from Example 0.4 by changing the word "correct" to "truistic." The resulting example satisfies all the Postulates P1–P6, P8–P11, but fails on P7 (since there are verdicts $a$ such that neither $a$ nor $a'$ is a "truistic" verdict).

Thus the distinction between an "*informal* Principia system with equality" and a "*formal* Principia system with equality" depends on the inclusion or rejection of Postulate P7.

It is important to observe, however, that another, equally good, example of a "formal Principia system with equality" is the system obtained from Example 0.5 by changing the word "incorrect" to "absurd." The mathematical postulates by themselves give no precedence to the "truistic-or" interpretation over the "absurd-and" interpretation.

† W. R. Hutcherson, *Maps of certain cyclic involutions on two-dimensional carriers*, this Bulletin, vol. 37 (1931), pp. 759–765.

$x_3+\epsilon\lambda x_4=0$ by $T$ and hence is non-invariant. The curve cut out on $F$ by $x_3+\lambda x_4=0$ is therefore non-invariant. The common tangent to the two curves is not transformed into itself. Hence the two curves do not touch each other at $P_2$. Since $C$ was a variable curve through $P_2$ satisfying the non-invariant property, it follows that $P_2$ is a non-perfect coincidence point. A similar argument shows that $P_1$, $P_3$, and $P_4$ are also non-perfect coincidence points. The following theorem has been proved.

THEOREM 1. *The $I_7$ belonging to $F_3$ in $S_3$ has four non-perfect points of coincidence.*

Consider the complete system of curves $|A|$ cut out on $F$ by all surfaces of order seven. Its dimension is 84, its genus is 64, and the number of variable intersections of two members of the system is 147. A curve $A$ of this system is not in general transformed into itself by $T$. There are, however, seven partial systems $|A_i|$ in $|A|$ which are transformed into themselves. By use of $|A_1|$ we find

$$a_1x_1^7 + a_2x_2^7 + a_3x_3^7 + a_4x_4^7 + a_5x_1^4x_2x_4^2 + a_6x_1^4x_3^2x_4 + a_7x_1^3x_2^2x_3x_4 + a_8x_1^3x_2x_3^3 + a_9x_1^2x_3x_4^4 + a_{10}x_1^2x_2^4x_4 + a_{11}x_1^2x_2^3x_3^2 + a_{12}x_1x_2x_3^2x_4^3 + a_{13}x_1x_2^2x_4^4 + a_{14}x_1x_3^4x_4^2 + a_{15}x_1x_2^5x_3 + a_{16}x_2x_3^5x_4 + a_{17}x_1^2x_3^2x_4^2 + a_{18}x_2^2x_3x_4^3 = 0.$$

We refer the curves $A_1$ projectively to the hyperplanes of a linear space of seventeen dimensions. We obtain a surface $\phi$, of order 21, with hyperplane sections of genus 10, as the image of $I_7$. The equations of the transformation for mapping $I_7$ upon $\phi$ in $S_{17}$ are

$$\begin{aligned}
\rho X_1 &= x_1^7, & \rho X_7 &= x_1^3x_2^2x_3x_4, & \rho X_{13} &= x_1x_2^2x_4^4,\\
\rho X_2 &= x_2^7, & \rho X_8 &= x_1^3x_2x_3^3, & \rho X_{14} &= x_1x_3^4x_4^2,\\
\rho X_3 &= x_3^7, & \rho X_9 &= x_1^2x_3x_4^4, & \rho X_{15} &= x_1x_2^5x_3,\\
\rho X_4 &= x_4^7, & \rho X_{10} &= x_1^2x_2^4x_4, & \rho X_{16} &= x_2x_3^5x_4,\\
\rho X_5 &= x_1^4x_2x_4^2, & \rho X_{11} &= x_1^2x_2^3x_3^2, & \rho X_{17} &= x_2^2x_3^2x_4^2,\\
\rho X_6 &= x_1^4x_3^2x_4, & \rho X_{12} &= x_1x_2x_3^2x_4^3, & \rho X_{18} &= x_2^3x_3x_4^3.
\end{aligned}$$

By eliminating $\rho, x_1, x_2, x_3, x_4$ from these eighteen equations and from $F_3(x_1x_2x_3x_4)=0$, we get as the fifteen equations defining the surface:

$$\begin{Vmatrix} X_1 & X_5 & X_8 & X_7 & X_6 \\ X_5 & X_{13} & X_{17} & X_{18} & X_{12} \end{Vmatrix} = 0, \quad \begin{Vmatrix} X_2 & X_{10} & X_{11} & X_{18} & X_{15} \\ X_{10} & X_5 & X_6 & X_9 & X_7 \end{Vmatrix} = 0,$$

$$\begin{Vmatrix} X_3 & X_{14} & X_{17} & X_{16} \\ X_{14} & X_9 & X_{13} & X_{12} \end{Vmatrix} = 0, \quad \begin{Vmatrix} X_4 & X_{13} & X_{12} \\ X_9 & X_7 & X_8 \end{Vmatrix} = 0, \quad \begin{Vmatrix} X_{18} & X_{12} \\ X_{17} & X_{14} \end{Vmatrix} = 0,$$

and $aX_{17}+bX_{14}+cX_{12}=0$. Designate by $P_2'$ the branch point of $\phi$ corresponding to the point $P_2$ on $F$. The coordinates of $P_2'$ are all zero except $X_2$.

The curves $A_1$ on $F$ pass through $P_2$ if $a_2=0$. The tangent plane at $P_2$ to $F$ is $x_3=0$. Now, the system of seventh-degree surfaces passing through $P_2$ cuts $x_3=0$ in the curves $x_3=0$, and

$$a_1x_1^7 + a_4x_4^7 + a_5x_1^4x_2x_4^2 + a_{10}x_1^2x_2^4x_4 + a_{13}x_1x_2^2x_4^4 = 0.$$

For general values of the constants this is a seventh-degree curve with a triple point at $P_2$, two branches being tangent to the line $x_1=x_3=0$ and one to the line $x_3=x_4=0$. When $a_5=a_{10}=a_{13}=0$, the plane seventh-degree curve breaks up into seven lines through $P_2$. These are all distinct except when either $a_1=0$ or $a_4=0$, when they coincide with $x_3=x_4=0$ or $x_1=x_3=0$, respectively. Since $P_2$ is non-perfect, the $|A_1|$ through $P_2$ must have seven distinct branches unless each branch touches one of the two invariant directions. In the plane $x_3=0$, the involution $I_7$ is generated by the homography $T_2$, which is

$$x_1' : x_2' : x_4' = x_1 : \epsilon x_2 : \epsilon^3 x_4.$$

By use of the plane quadratic transformation $X$: $y_1:y_2:y_4 = w_1w_4 : w_2^2 : w_1w_2$ and its inverse $X^{-1}$: $w_1:w_2:w_4 = y_4^2 : y_2y_4 : y_1y_2$ as well as the transformation $Y$: $y_1:y_2:y_4 = w_2w_4 : w_2^2 : w_1w_4$ and its inverse $Y^{-1}$: $w_1:w_2:w_4 = y_2y_4 : y_1y_2 : y_1^2$, we can investigate the character of the adjacent invariant points along the two invariant directions at $P_2$. By the application of $XT_2X^{-1} \equiv T_2'$,

$$(w_1,w_2,w_4) \overset{X^{-1}}{\sim} (y_4^2, y_2y_4, y_1y_2) \overset{T_2}{\sim} (\epsilon^6y_4^2, \epsilon^4y_2y_4, \epsilon y_1y_2),$$

or

$$(\epsilon^5y_4^2, \epsilon^3y_2y_4, y_1y_2) \overset{X}{\sim} (\epsilon^5w_1, \epsilon^3w_2, w_4).$$

Thus the new transformation $T_2'$ is $x_1' : x_2' : x_4' = \epsilon^5x_1 : \epsilon^3x_2 : x_4$. The invariant point adjacent to $P_2$ along the line $x_1=x_3=0$ is still a non-perfect coincidence point. Using on the next point

$YT_2'Y^{-1} \equiv T_2''$, we find $(w_1, w_2, w_4) \underset{T_2'}{\sim} (w_1, \epsilon^5 w_2, w_4)$. This point is a perfect point of coincidence. This means that $T_2''$ is $x_1' : x_2' : x_4' = x_1 : \epsilon^5 x_2 : x_4$ and hence it is the collineation representing a perfect point for (0, 1, 0). Thus, by $XT_2X^{-1}$ and $YT_2'Y^{-1}$, one finds a perfect point along $x_1 = x_3 = 0$ in the neighborhood of the second order of $P_2$. Therefore the following is true.

THEOREM 2. *Along the invariant direction $x_1 = x_3 = 0$, the invariant point $P_2$ has an imperfect point in the first-order neighborhood and a perfect one in the second-order neighborhood.*

Next, investigate the characteristics of the adjacent point to $P_2$ along the invariant direction $x_3 = x_4 = 0$. By use of $YT_2Y^{-1} \equiv T_2^{(1)}$ we get

$$(w_1, w_2, w_4) \underset{\sim}{Y^{-1}} (x_2x_4, x_1x_2, x_1^2) \underset{\sim}{T_2} (\epsilon^4 x_2x_4, \epsilon x_1x_2, x_1^2)$$

$$\underset{\sim}{Y} (\epsilon^4 w_1, \epsilon w_2, w_4).$$

Hence $T_2^{(1)}$ is $x_1' : x_2' : x_4' = \epsilon^4 x_1 : \epsilon x_2 : x_4$ and this indicates an imperfect point adjacent to $P_2$ along $x_3 = x_4 = 0$. Apply $Y\ T_2'\ Y^{-1} \equiv T_2^{(11)}$ and find $(w_1, w_2, w_4) \sim (w_1, \epsilon^4 w_2, w_4)$. Since $T_2^{(11)}$ becomes $x_1' : x_2' : x_4' = x_1 : \epsilon^4\ x_2 : x_4$, we are assured of a perfect point in the second-order neighborhood of $P_2$ along this invariant direction. Hence the theorem follows.

THEOREM 3. *Along the invariant direction $x_4 = x_3 = 0$, the invariant imperfect point $P_2$ has an imperfect point in the first-order neighborhood and a perfect one in the second-order neighborhood.*

The following theorem is now self-evident.

THEOREM 4. *The imperfect point $P_2$ on $F_3$ has no perfect points in the neighborhood of the first order but precisely two perfect ones in the neighborhood of the second order.*

The tangent plane to $F$ at $P_3 \equiv (0, 0, 1, 0)$ is $x_1 = 0$. The homography $T_3$ in $x_1 = 0$ is $x_2' : x_3' : x_4' = x_2 : \epsilon x_3 : \epsilon^2 x_4$. To investigate the adjacent points to $P_3$ along the two invariant directions $x_1 = x_2 = 0$ and $x_1 = x_4 = 0$, one needs the following two quadratic transformations and their inverses:

$$\begin{aligned}
Y_1: &\quad y_2 : y_3 : y_4 = w_3w_4 : w_3^2 : w_2w_4, \\
Y_1^{-1}: &\quad w_2 : w_3 : w_4 = y_2y_4 : y_2y_3 : y_2^2, \\
X_1: &\quad y_2 : y_3 : y_4 = w_2w_4 : w_3^2 : w_2w_3, \\
X_1^{-1}: &\quad w_2 : w_3 : w_4 = y_3^2 : y_3y_4 : y_2y_3.
\end{aligned}$$

Apply $X_1T_3X_1^{-1} \equiv T_3'$ along $x_1 = x_4 = 0$ adjacent to $P_3$. Then we have

$$(w_2, w_3, w_4) \overset{X_1^{-1}}{\sim} (y_4^2, y_3y_4, y_2y_3) \overset{T_3}{\sim} (\epsilon^2 y_4^2, \epsilon^3 y_3y_4, \epsilon y_2y_3)$$

$$\overset{X_1}{\sim} (\epsilon w_2, \epsilon^2 w_3, w_4).$$

Since $T_3'$ is $x_2' : x_3' : x_4' = \epsilon x_2 : \epsilon^2 x_3 : x_4$, we have an imperfect point. By using $Y_1T_3'Y_1^{-1} = T_3''$, we get

$$(w_2, w_3, w_4) \overset{T_3''}{\sim} (\epsilon^2 w_2, \epsilon^3 w_3, \epsilon^2 w_4).$$

Hence we have a perfect point.

THEOREM 5. *Along the invariant direction $x_1 = x_2 = 0$, the invariant imperfect point $P_3$ has an imperfect adjacent point and a perfect one in the neighborhood of the second order.*

Now consider the possibilities along $x_1 = x_4 = 0$, the other invariant direction. Apply $Y_1T_3Y_1^{-1} \equiv T_3^{(I)}$ and get

$$(w_2, w_3, w_4) \sim (\epsilon^3 w_2, \epsilon w_3, w_4),$$

which signifies an imperfect point. Applying $Y_1T_3^{(I)}Y_1^{-1} \equiv T_3^{(II)}$, we get $(w_2, w_3, w_4) \sim (w_2, \epsilon^2 w_3, \epsilon^5 w_4)$, another imperfect point. By use of $X_1T_3^{(II)}X_1^{-1} = T_3^{(III)}$, we get $(w_2, w_3, w_4) \sim (\epsilon^2 w_2, \epsilon w_3, \epsilon^2 w_4)$, which indicates that $T_3^{(III)}$ is $x_2' : x_3' : x_4' = \epsilon^2 x_2 : x_3 : \epsilon^2 x_4$. Hence we have found a perfect point, and the theorem follows.

THEOREM 6. *Along the invariant direction $x_1 = x_4 = 0$, the invariant imperfect point $P_3$ has no perfect points in the first- and second-order neighborhoods but does have one in the third-order neighborhood.*

3. *Sections by Sextics.* Consider the complete system of curves $|B|$ cut out on $F$ by all surfaces of order six. Its dimension is 63, its genus is 46, and the number of variable intersections of two members of the system is 108. A curve $B$ of this system is not in general transformed into itself. There are, however, seven partial systems $|B_i|$ in $|B|$ which are transformed into themselves. By use of $|B_1|$ we find

$$b_1x_1x_4^5 + b_2x_2x_3x_4^4 + b_3x_3^3x_4^3 + b_4x_1^2x_2^2x_4^2 + b_5x_1^3x_3x_4^2 + b_6x_2^5x_4$$
$$+ b_7x_1x_2^3x_3x_4 + b_8x_1^2x_2x_3^2x_4 + b_9x_1^2x_3^4 + b_{10}x_1x_2^2x_3^3$$
$$+ b_{11}x_2^4x_3^2 + b_{12}x_1^5x_2 = 0.$$

If we refer the curves $B_1$ projectively to the hyperplanes of a

linear space of eleven dimensions, we obtain a surface $\phi$. The equations of transformation for mapping $I_7$ upon $\phi$ in $S_{11}$ are

$$\begin{aligned}
\rho X_1 &= x_1 x_4^5, & \rho X_5 &= x_1^3 x_3 x_4^2, & \rho X_9 &= x_1^2 x_3^4,\\
\rho X_2 &= x_2 x_3 x_4^4, & \rho X_6 &= x_2^5 x_4, & \rho X_{10} &= x_1 x_2^2 x_3^3,\\
\rho X_3 &= x_3^3 x_4^3, & \rho X_7 &= x_1 x_2^3 x_3 x_4, & \rho X_{11} &= x_2^4 x_3^2,\\
\rho X_4 &= x_1^2 x_2^2 x_4^2, & \rho X_8 &= x_1^2 x_2 x_3^2 x_4, & \rho X_{12} &= x_1^5 x_2.
\end{aligned}$$

By eliminating $\rho$, $x_1$, $x_2$, $x_3$, $x_4$ from these twelve equations and from $F_3(x_1,x_2,x_3,x_4)=0$, we get as the nine equations defining the surface

$$\left\| \begin{matrix} X_1 & X_4 & X_7 \\ X_2 & X_7 & X_{11} \end{matrix} \right\| = 0, \quad \left\| \begin{matrix} X_4 & X_7 & X_6 \\ X_8 & X_{10} & X_{11} \end{matrix} \right\| = 0,$$

$$\left\| \begin{matrix} X_7 & X_{10} & X_6 \\ X_8 & X_9 & X_7 \end{matrix} \right\| = 0, \quad \left\| \begin{matrix} X_5 & X_2 & X_3 \\ X_{12} & X_4 & X_8 \end{matrix} \right\| = 0,$$

and $aX_7+bX_8+cX_4=0$.

All the curves $B_1$ pass through the invariant points $P_1$, $P_2$, $P_3$, $P_4$. Consider point $P_2$. Its tangent plane is $x_3=0$. It cuts the sextic surfaces in the curves

$$x_3 = 0,\ b_1 x_1 x_4^5 + b_4 x_1^2 x_2^2 x_4^2 + b_6 x_2^5 x_4 + b_{12} x_1^5 x_2 = 0.$$

This curve passes simply through $P_2$ along the invariant direction $x_3=x_4=0$. If $b_6=0$, the curve degenerates into a line and a quintic with a triple point formed by a simple branch passing through a cusp. The line is the simple tangent at the triple point, while the cuspidal tangent cuts the curve again at an undulation. If $b_6=b_4=0$, the curve degenerates into a quintic with a five-fold point (having five coincident tangents) and a line, the tangent at the five-fold point. If $b_6=b_4=b_{12}=0$, $P_2$ is a six-fold point. The curve breaks up into six lines, one of which is $x_1=x_3=0$, while the other five are $x_3=x_4=0$ counted five times. Thus the system of $B_1$ curves passes through $P_2$ along invariant directions.

The tangent plane at $P_3$ is $x_1=0$. It cuts the sextic surfaces in the curves $x_1=0$, $b_2x_2x_3x_4^4+b_3x_3^3x_4^3+b_6x_2^5x_4+b_{11}x_2^4x_3^2=0$. $P_3$ is a special triple point on these curves having three coincident tangents. The curves touch at $P_3$ along the invariant direction $x_1=x_4=0$. If $b_3=0$, then the curve passes through $P_3$ four times and is tangent to $x_1=x_2=0$ four times. When $b_3=b_{11}=0$, the

curve is five fold at $P_3$, passing through along the invariant direction $x_1=x_2=0$ once and along $x_1=x_4=0$ four times. When $b_3=b_{11}=b_2=0$, the curve breaks up into six lines through $P_3$, namely, $x_1=x_4=0$ counted simply and $x_1=x_2=0$ counted five times. The following theorem may be stated.

THEOREM 7. *The* $|B_1|$ *curves pass through the imperfect points only along the invariant directions.*

4. *Sections by Quintics.* The complete system of curves $|C|$ cut out on $F$ by all surfaces of order five has dimension 45, genus 31, and the number of variable intersections of two members of the system is 75. There are seven partial systems $|C_i|$ in $|C|$ which are transformed into themselves. By the use of $|C_1|$ we find

$$c_1x_1^2x_4^3 + c_2x_1x_2x_3x_4^2 + c_3x_2^3x_4^2 + c_4x_1x_3^3x_4 + c_5x_2^2x_3^2x_4 + c_6x_2x_3^4 + c_7x_1^4x_3 + c_8x_1^3x_2^2 = 0.$$

By referring the curves $C_1$ projectively to the hyperplanes of a linear space of seven dimensions, we obtain a surface $\phi$. The equations of transformation for mapping $I_7$ upon $\phi$ in $S_7$ are

$$\rho X_1 = x_1^2x_4^3, \quad \rho X_3 = x_2^3x_4^2, \quad \rho X_5 = x_2^2x_3^2x_4, \quad \rho X_7 = x_1^4x_3,$$
$$\rho X_2 = x_1x_2x_3x_4^2, \quad \rho X_4 = x_1x_3^3x_4, \quad \rho X_6 = x_2x_3^4, \quad \rho X_8 = x_1^3x_2^2.$$

Eliminate $\rho$, $x_1$, $x_2$, $x_3$, $x_4$ from these eight equations and from $F_3(x_1, x_2, x_3, x_4)=0$. The five equations defining the surface $\phi$ are

$$\begin{Vmatrix} X_1 & X_2 & X_4 \\ X_2 & X_5 & X_6 \end{Vmatrix} = 0, \quad \begin{Vmatrix} X_3 & X_5 \\ X_5 & X_6 \end{Vmatrix} = 0, \quad \begin{Vmatrix} X_2 & X_7 \\ X_3 & X_8 \end{Vmatrix} = 0,$$

and

$$aX_5 + bX_4 + cX_2 = 0.$$

All the curves $C_1$ pass through the invariant points $P_1$, $P_2$, $P_3$, $P_4$. Its tangent plane at $P_2$ is $x_3=0$. It cuts the quintic surfaces in the curves $x_3=0$, $c_1x_1^2x_4^3+c_3x_2^3x_4^2+c_8x_1^3x_2^2=0$. This curve has a double point at $P_2$, both branches being tangent to the invariant direction $x_3=x_4=0$. When $c_3=0$, the curve degenerates into a cuspidal cubic and a repeated line (the flex tangent, which is $x_1=x_3=0$). If $c_3=c_8=0$, the curve degenerates into five straight lines through $P_2$. They are $x_1=x_3=0$ counted twice and

$x_3=x_4=0$ counted three times. Hence these curves pass through $P_2$ along invariant directions.

The tangent plane to $F_3$ at $P_3$ is $x_1=0$. It cuts the quintic surfaces in the curves $x_1=0$, $c_3x_2^3x_4^2+c_5x_2^2x_3^2x_4+c_6x_2x_3^4=0$. This curve is simple at $P_3$, passing through along the invariant direction $x_1=x_2=0$. When $c_6=0$, the curve degenerates into a conic and three lines, one line $(x_1=x_4=0)$ a simple tangent and the other $(x_1=x_2=0)$ a repeated tangent. If $c_6=c_5=0$, then the curve breaks up into the line $x_1=x_2=0$ counted three times and the line $x_1=x_4=0$ counted twice.

THEOREM 8. *The* $|C_1|$ *curves pass through imperfect points only along invariant directions.*

5. *Sections by Quartics.* The dimension of the complete system of curves $|D|$ cut out on $F$ by all surfaces of order four is 30, its genus is 19, and the number of variable intersections of two members of the system is 48. By use of $|D_1|$ we find

$$d_1x_2x_4^3+d_2x_3^2x_4^2+d_3x_1^3x_4+d_4x_1x_2^3+d_5x_1^2x_2x_3=0.$$

We refer the curves $D_1$ projectively to the hyperplanes of a linear space of four dimensions, and obtain a surface $\phi$. The equations of transformation for mapping $I_7$ upon $\phi$ in $S_4$ are

$$\rho X_1=x_2x_4^3,\ \rho X_2=x_3^2x_4^2,\ \rho X_3=x_1^3x_4,\ \rho X_4=x_1x_2^3,$$

$$\rho X_5=x_1^2x_2x_3.$$

The two equations defining the surface are

$$X_1X_5^2=X_2X_3X_4 \quad \text{and} \quad aX_1X_5+bX_2X_3+cX_1X_3=0.$$

All the curves $D_1$ pass through the invariant points $P_1$, $P_2$, $P_3$, and $P_4$. Consider the point $P_2$. Its tangent plane is $x_3=0$. It cuts the quartic surfaces in the curves

$$x_3=0,\ d_1x_2x_4^3+d_3x_1^3x_4+d_4x_1x_2^3=0.$$

This curve passes simply through $P_2$ along the $x_1=x_3=0$ direction. When $d_4=0$, the curve degenerates into a cuspidal cubic and the cusp tangent $(x_3=x_4=0)$. When $d_4=d_1=0$, the curve breaks up into four lines through $P_2$. They are $x_1=x_3=0$ counted three times and $x_3=x_4=0$ counted once.

The tangent plane at $P_3$ cuts the quartic surfaces in the curves $x_1=0$, $d_1x_2x_4^3+d_2x_3^2x_4^2=0$. The quartic curves degenerate into

conics and a repeated (tangent) line. When $d_2=0$, they break up into $x_1=x_4=0$ counted three times and $x_1=x_2=0$ counted once.

THEOREM 9. *The* $|D_1|$ *curves pass through imperfect points only along invariant directions.*

6. *Sections by Cubics.* Investigate the complete system of curves $|E|$ cut out on $F$ by all surfaces of order three. Its dimension is 19, genus is 10, and the number of variable intersections of the two members of the system is 27. The use of $|E_1|$ gives $e_1x_2^2x_3+e_2x_1x_3^2+e_3x_1x_2x_4=0$. The equations of transformation for referring the curves $E_1$ projectively to the lines of a plane are $\rho X_1=x_2^2x_3$, $\rho X_2=x_1x_3^2$, $\rho X_3=x_1x_2x_4$. A curve $aX_1+bX_2+cX_3=0$ is obtained, instead of a surface. All the curves $E_1$ pass through the invariant points $P_1$, $P_2$, $P_3$, and $P_4$. The tangent plane to $F_3$ at $P_2$ is $x_3=0$. This intersects $E_1$ surfaces in $x_3=0$, $x_1x_2x_4=0$. Hence, the cubic curve becomes three straight lines, two of which pass through $P_2$, namely, $x_1=x_3=0$ and $x_3=x_4=0$. At $P_3$ the tangent plane is $x_1=0$. It cuts the $E_1$ surfaces in $x_1=0$, $x_2^2x_3=0$. This degenerate cubic curve also has a double point at $P_3$. The branches are $x_1=x_2=0$ counted twice. Hence the following theorem is proved.

THEOREM 10. *The system of invariant curves cut out upon F by surfaces of degree lower than seven all pass through the coincidence points along the invariant directions. The number of branches through each point is less than seven.*

BEREA COLLEGE

# NOTE ON RELATIONS CONNECTING CERTAIN CASES OF CONVERGENCE IN THE MEAN*

BY DUNHAM JACKSON

1. *Introduction.* A lemma from which various inferences can be drawn with regard to the convergence of sequences of trigonometric sums reads as follows.†

LEMMA A. *If $f(x)$ is a continuous function of period $2\pi$, $T_n(x)$ a trigonometric sum of the nth order, and*

$$G_{ns} = \int_{-\pi}^{\pi} |f(x) - T_n(x)|^s dx,$$

*and if there exists a trigonometric sum $t_n(x)$ of the nth order such that $|f(x)-t_n(x)| \leqq \epsilon_n$ everywhere, then*

$$|f(x) - T_n(x)| \leqq 4(nG_{ns})^{1/s} + 5\epsilon_n$$

*for all values of $x$.*

The exponent $s$ may be any positive constant. In view of the continuity of $f(x)$, it is possible to construct approximating sums $t_n(x)$ for successive values of $n$ and to assign corresponding upper bounds $\epsilon_n$ for the error of the approximation so that $\lim_{n\to\infty}\epsilon_n = 0$. It follows as an immediate corollary of the lemma that if a sequence of sums $T_n(x)$ has the property that $\lim_{n\to\infty} nG_{ns} = 0$, for fixed $s$, then $T_n(x)$ converges uniformly toward $f(x)$ as $n$ becomes infinite. This may be regarded as constituting a relationship between the convergence properties of two measures of the discrepancy between $f(x)$ and the sum $T_n(x)$, regarded as an approximation to $f(x)$: the mean value $G_{ns}/(2\pi)$ of the $s$th power of the error, and the maximum value attained by the error at any single point. The latter will converge to zero if the former approaches zero *with sufficient rapidity*. On the other hand, if the maximum error approaches zero, the mean will necessarily approach zero, without further restriction.

---

* Presented to the Society, December 27, 1933.

† See D. Jackson, *Certain problems of closest approximation*, this Bulletin vol. 39 (1933), pp. 889–908, Lemma 5.

The aim of this paper is to point out corresponding relations between the properties of convergence of the means corresponding to two different exponents $s$ and $\sigma$. One side of the relationship is an obvious consequence of Hölder's inequality; the other is recognizable as a simple corollary of the lemma. As would naturally be expected, the result corresponding to the use of the maximum error as measure of the discrepancy is approached as a limit if $\sigma$ is allowed to become infinite. For the purpose in hand the lemma as first stated will be replaced by a slightly modified version, which is not effective for the proof of uniform convergence but admits consideration of discontinuous functions in the treatment of convergence in the mean. It may be emphasized that except when expressly noted below no *minimizing* property need be ascribed to the sums $T_n(x)$; they are not necessarily determined by any criterion of closest approximation.

To the discussion of trigonometric approximation there corresponds a parallel treatment of approximation by means of polynomials, which will, however, not be carried through in detail.

The principle is illustrated in exceedingly simple form by a problem which may be regarded as a special case of the preceding for $f(x) \equiv 0$, but is more directly of interest for its own sake. This special problem will be treated first.

2. *Integrals of Powers of Trigonometric Sums and Polynomials.* If $\phi(x)$ is a non-negative function over an interval $(a, b)$, and if the value of the integral

$$H_s = \int_a^b [\phi(x)]^s dx$$

is known, an upper bound for the magnitude of the integral $H_\sigma$ with a value of $\sigma < s$ is given by Hölder's inequality. For $\sigma > s$ no such upper bound is in general available. For special classes of functions $\phi(x)$, however, a relation of inequality giving an upper bound is obtainable in this case also.

Let $T_n(x)$ be a trigonometric sum of the $n$th order, and let

$$H_{ns} = \int_{-\pi}^{\pi} |T_n(x)|^s dx,$$

with an arbitrary positive exponent $s$. For $\sigma < s$, by Hölder's

inequality, $H_n \leqq (2\pi)^{1-(\sigma/s)}(H_{ns})^{(\sigma/s)}$. The following lemma, the proof of which* (like that of Lemma A) depends on Bernstein's theorem on the derivative of a trigonometric sum, leads at once to the desired inequality in the contrary case.

LEMMA B. *If $T_n(x)$ is a trigonometric sum of the nth order, if*

$$H_{ns} = \int_{-\pi}^{\pi} |T_n(x)|^s dx,$$

*and if $\lambda_n$ is the maximum of $|T_n(x)|$, then $\mu_n \leqq 2(nH_{ns})^{1/s}$.*

If $\sigma > s$, application of this lemma gives

$$H_{n\sigma} = \int_{-\pi}^{\pi} |T_n(x)|^{\sigma-s} |T_n(x)|^s dx$$
$$\leqq [2(nH_{ns})^{1/s}]^{\sigma-s} H_{ns} = 2^{\sigma-s} n^{(\sigma/s)-1} (H_{ns})^{\sigma/s}.$$

The result involves the order of the trigonometric sum through the factor $n^{(\sigma/s)-1}$. The inequality can be written in the more symmetrical form

$$(nH_{n\sigma})^{1/\sigma} \leqq 2^{1-(s/\sigma)}(nH_{ns})^{1/s}.$$

Similarly, if $P_n(x)$ is a polynomial of the $n$th degree, and

$$H_{ns} = \int_a^b |P_n(x)|^s dx,$$

then

$$H_{n\sigma} \leqq (b-a)^{1-(\sigma/s)}(H_{ns})^{\sigma/s}$$

for $\sigma < s$, by Hölder's inequality, and

$$H_{n\sigma} \leqq C^\sigma n^{2(\sigma-s)/s}(H_{ns})^{\sigma/s}, \quad (n^2 H_{n\sigma})^{1/\sigma} \leqq C(n^2 H_{ns})^{1/s},$$

for $\sigma > s$, in consequence of a proposition† analogous to Lemma B, the constant $C$ having the value $\{2[4/(b-a)]^{1/s}\}^{(\sigma-s)/\sigma}$.

3. *Convergence of Trigonometric Approximation.* Let $f(x)$ be a given function of period $2\pi$ which is bounded and integrable (in the sense of Riemann or in the sense of Lebesgue), and let $T_n(x)$ be a trigonometric sum of the $n$th order. Let

---

* See this Bulletin, loc. cit., Lemma 1.

† See this Bulletin, loc. cit., Lemma 2.

$$G_{ns} = \int_{-\pi}^{\pi} |f(x) - T_n(x)|^s dx$$

with any value of $s>0$. If $\sigma<s$, application of Hölder's inequality gives

$$G_{n\sigma} \leqq (2\pi)^{1-(\sigma/s)}(G_{ns})^{\sigma/s}.$$

It follows that if a sequence of sums $T_n(x)$ is given so that $\lim_{n\to\infty} G_{ns}=0$ for a fixed value of $s$, then $\lim_{n\to\infty} G_{n\sigma}=0$ for any fixed $\sigma<s$.

For treatment of the case $\sigma>s$ the following modification of Lemma A will be established.

LEMMA C. *If $f(x)$ is a bounded and integrable function of period $2\pi$ having $M$ as an upper bound for its absolute value, $T_n(x)$ a trigonometric sum of the nth order, and*

$$G_{ns} = \int_{-\pi}^{\pi} |f(x) - T_n(x)|^s dx,$$

*then*

$$|f(x) - T_n(x)| \leqq 4(nG_{ns})^{1/s} + 5M$$

*for all values of $x$.*

Let $\mu_n$ be the maximum of $|T_n(x)|$, attained for $x=x_0$. By Bernstein's theorem, $|T_n'(x)| \leqq n\mu_n$ everywhere. For $|x-x_0| \leqq 1/(2n)$, $|T_n(x_0)-T_n(x)| \leqq \mu_n/2$, and $|T_n(x)| \geqq \mu_n/2$. If $\mu_n \geqq 4M$, so that $|f(x)| \leqq \mu_n/4$, then $|f(x)-T_n(x)| \geqq \mu_n/4$ throughout the specified range of values for $x$. The length of the interval being $1/n$,

$$G_{ns} \geqq \frac{1}{n}\left(\frac{\mu_n}{4}\right)^s,$$

so that $\mu_n \leqq 4(nG_{ns})^{1/s}$. If $\mu_n<4M$, this inequality in itself serves to give an upper bound for $\mu_n$. In any case $\mu_n$ can not exceed the sum of the two alternative upper bounds:

$$|T_n(x)| \leqq \mu_n \leqq 4(nG_{ns})^{1/s} + 4M.$$

Combination of this relation with the fact that $|f(x)| \leqq M$ gives the conclusion of the lemma.

If $\sigma>s$, it is seen by application of the lemma that

$$G_{n\sigma} \leqq [4(nG_{ns})^{1/s} + 5M]^{\sigma-s} G_{ns}.$$

Hence

$$(G_{n\sigma})^{1/(\sigma-s)} \leqq [4(nG_{ns})^{1/s} + 5M](G_{ns})^{1/(\sigma-s)}$$
$$= 4[n^{1-(s/\sigma)}G_{ns}]^{\sigma/[s(\sigma-s)]} + 5M(G_{ns})^{1/(\sigma-s)}.$$

If the given sums $T_n(x)$ are such that $n^{1-(s/\sigma)}G_{ns}$ approaches zero, $G_{ns}$ by itself will approach zero a fortiori, the whole right-hand member will converge toward zero, and the same will be true of $G_{n\sigma}$. *For convergence of $G_{n\sigma}$ toward zero as $n$ becomes infinite, when $\sigma > s$, it is sufficient that*

$$\lim_{n\to\infty} n^{1-(s/\sigma)}G_{ns} = 0.$$

Although it has not been required in the preceding general argument that the sums $T_n(x)$ possess any minimizing property, the reasoning applies in particular if $T_n(x)$ is characterized among all trigonometric sums of the $n$th order as one for which $G_{ns}$ has the smallest possible value.

For example, if $T_n(x)$ is the partial sum of the Fourier series for $f(x)$ through the terms in $\cos nx$ and $\sin nx$, and if $f(x)$ is of limited variation, $\lim_{n\to\infty} G_{n\sigma} = 0$ for every positive value of $\sigma$. For

$$G_{n2} = \pi \sum_{k=n+1}^{\infty} (a_k^2 + b_k^2),$$

where $a_k$ and $b_k$ are the Fourier coefficients of $f(x)$; these coefficients have an upper bound of the order of $1/k$; and $G_{n2}$ consequently has an upper bound of the order of $1/n$. The same conclusion with regard to the convergence of $G_{n\sigma}$ can also be reached in other ways.

As another illustration, let it be supposed that $f(x)$ is continuous, and that a trigonometric sum $t_n(x)$ of the $n$th order exists so that $|f(x) - t_n(x)| \leqq \epsilon_n$ for all values of $x$. If $T_n(x)$ is a sum which minimizes $G_{ns}$, then by virtue of this minimizing property

$$G_{ns} = \int_{-\pi}^{\pi} |f(x) - T_n(x)|^s dx \leqq \int_{-\pi}^{\pi} |f(x) - t_n(x)|^s dx \leqq 2\pi\epsilon_n^s.$$

A sufficient condition for the convergence of $G_{n\sigma}$ toward zero as $n$ becomes infinite, when $s$ and $\sigma$ are held fast and the sums

$T_n(x)$ are chosen each time to minimize $G_{ns}$, is that sums $t_n(x)$ exist for the successive values of $n$ so that

$$\lim_{n\to\infty} n^{1-(s/\sigma)}\epsilon_n{}^s = 0, \qquad \lim_{n\to\infty} n^{(1/s)-(1/\sigma)}\epsilon_n = 0.$$

This condition will be fulfilled,* when $(1/s)-(1/\sigma)<1$, if $f(x)$ has a modulus of continuity $\omega(\delta)$ such that

$$\lim_{\delta\to 0} \omega(\delta)/\delta^{(1/s)-(1/\sigma)} = 0.$$

The case of Fourier series is included for $s=2$. This special case, however, can be treated more advantageously by a different method. If $T_n(x)$ is the partial sum of the Fourier series, and if a trigonometric sum $t_n(x)$ of the $n$th order exists with $\epsilon_n$ as an upper bound for the difference $|f(x)-t_n(x)|$, then†

$$|f(x) - T_n(x)| \leqq B\epsilon_n \log n$$

for all values of $x$, where $B$ is an absolute constant. By the least-square property of the Fourier series,

$$G_{n2} \leqq \int_{-\pi}^{\pi} [f(x) - t_n(x)]^2 dx \leqq 2\pi\epsilon_n^2,$$

and for $\sigma>2$

$$G_{n\sigma} \leqq (B\epsilon_n \log n)^{\sigma-2}G_{n2} \leqq 2\pi B^{\sigma-2}(\log n)^{\sigma-2}\epsilon_n{}^{\sigma},$$

so that $G_{n\sigma}$ will approach zero if $\lim_{n\to\infty} (\log n)^{1-(2/\sigma)}\ \epsilon_n=0$, and hence if

$$\lim_{\delta\to 0} (\log \delta)^{1-(2/\sigma)}\omega(\delta) = 0,$$

where $\omega(\delta)$ is the modulus of continuity of $f(x)$.

For general $s$ and for $(1/s)-(1/\sigma)\geqq 1$, sufficient conditions for convergence can be formulated in terms of the existence and properties of continuity of one or more derivatives‡ of $f(x)$.

* See for example the writer's *Theory of Approximation*, Colloquium Publications of this Society, vol. 11, 1930, p. 7, Theorem 2.

† See for example the Colloquium cited in the preceding footnote, p. 21, Theorem 9; H. Lebesgue, *Sur la représentation trigonométrique approchée des fonctions satisfaisant à une condition de Lipschitz*, Bulletin de la Société Mathématique de France, vol. 38 (1910), pp. 184–210; pp. 196–197, 201.

‡ See Colloquium, p. 12, Theorem 4.

Conditions for the convergence of $G_{ns}$ in terms of the order of magnitude of $\epsilon_n$ can be stated without change of form if $T_n(x)$, instead of minimizing $G_{ns}$, is chosen so as to reduce the integral

$$\int_{-\pi}^{\pi} \rho(x)\left|f(x) - T_n(x)\right|^s dx$$

to a minimum, where $\rho(x)$ is a summable function having a positive lower bound. Similar statements, with a modification of the exponent of the power of $n$, can be made in certain cases when the greatest lower bound of $\rho(x)$ is zero.*

These conclusions relating specifically to sums $T_n(x)$ which possess a minimizing property are almost immediate consequences of results previously published as to the order of magnitude of $f(x)-T_n(x)$, and have the force of corollaries, pointing out implications already present in those results.

4. *Lemma for the Case of Polynomial Approximation.* Explicit treatment of polynomial approximation will be confined here to the formulation of an analog of Lemma C.

LEMMA D. *If $f(x)$ is a bounded and integrable function over the interval $(a, b)$, with $M$ as an upper bound for its absolute value, if $P_n(x)$ is a polynomial of the nth degree, and if*

$$G_{ns} = \int_a^b \left|f(x) - P_n(x)\right|^s dx,$$

*then*

$$\left|f(x) - P_n(x)\right| \leqq 4\left(\frac{4n^2 G_{ns}}{b-a}\right)^{1/s} + 5M$$

*for $a \leqq x \leqq b$.*

The proof is similar to that of Lemma C, with use of Markoff's theorem in place of that of Bernstein.

THE UNIVERSITY OF MINNESOTA

* See this Bulletin, loc. cit., Theorems 9 and 10.

# CONCERNING MAXIMAL SETS*

BY G. T. WHYBURN

1. *Introduction.* Let $T$ be any monotone system of closed subsets of an arbitrary metric space $M$, that is, any closed subset of a set of the system $T$ is itself a set of $T$. We shall call a set of the system $T$ a *$T$-set* or a *set of type $T$*. We may also think of $T$ as a property such that every closed subset of a set having this property likewise has this property.

Since the null set (0) is a subset of every set, then, whatever be the system $T$, the null set is always a $T$-set.

We first establish a general existence theorem for certain maximal sets relative to a system $T$.

2. THEOREM. *If $N$ is any closed non-degenerate subset of a metric space $M$ such that $N$ is not disconnected by the omission of any $T$-set, then there exists a maximal subset (a continuum) $H(N)$ of $M$ containing $N$ and having this property.*

PROOF. In the first place, $N$ is connected, since $N-(0)$ is connected and is identical with $N$.

Secondly, $N$ is not a $T$-set, for if it were then every closed subset of $N$ would likewise be a $T$-set, and clearly some closed subset of $N$ disconnects $N$.

Now if $H$ denotes the sum of all sets $N_0$ containing $N$ and such that $N_0$ is not disconnected by the omission of any $T$-set, then clearly $H$ is connected and hence $\overline{H}$ is a continuum.

We proceed to show that no $T$-set disconnects $\overline{H}$. Suppose on the contrary, that we have a separation $\overline{H}-T=H_1+H_2$, where $T$ is some $T$-set in $\overline{H}$. Then $N-N\cdot T$ is connected and thus is contained wholly in one of the sets $H_1$ and $H_2$, say $H_1$. But $H\cdot H_2$ contains at least one point $x$, since $H_2$ is open in $\overline{H}$. There exists a continuum $N_x$ in $H$ containing $x+N$ and such that $N_x$ is not disconnected by any $T$-set. But $N_x\cdot T$ is a $T$-set and we have a separation

$$N_x - N_x\cdot T = N_x\cdot H_1 + N_x\cdot H_2,$$

and both sets of the right hand member are non-vacuous since

* Presented to the Society, October 28, 1933.

$H_2 \supset x$ and $H_1 \cdot N_x \supset (N - N \cdot T)$. Thus the supposition that $\overline{H}$ is disconnected by the omission of some $T$-set leads to a contradiction.

Consequently we have only to set $H(N) = \overline{H}$, and our theorem is established.

3. THEOREM. *The common part of any two sets $H(N)$ is a $T$-set.*

For let $H(N_1) \neq H(N_2)$ and suppose $H(N_1) \cdot H(N_2) \neq 0$, the other case being trivial. Set $H(N_1) + H(N_2) = H$. There exists a $T$-set $T$ in $H$ such that we have a separation $H - T = H_1 + H_2$. Now $H(N_1) - T \cdot H(N_1)$ and $H(N_2) - T \cdot H(N_2)$ are connected, since the sets taken away are $T$-sets. Hence $T \supset H(N_1) \cdot H(N_2)$, for if not then the set

$$[H(N_1) - T \cdot H(N_1)] + [H(N_2) - T \cdot H(N_2)]$$
$$= H(N_1) + H(N_2) - T = H - T$$

is connected. Thus $H(N_1) \cdot H(N_2)$ is a $T$-set, since it is a subset of $T$.

4. *Applications.* (i) Let $T$ be the property of being the null set. Then the corresponding sets $H(N)$ given by §2 are the components of $M$.

(ii) Let $T$ be the property of containing at most $n$ points, $(n = 0, 1, 2, \cdots)$.

For $n = 0$, we have the case just considered under (i). For $n = 1$, we obtain for $H(N)$ subcontinua of $M$ which are maximal with respect to the property of having no cut point.* In case $M$ is a locally connected continuum, these sets $H(N)$ are the true cyclic elements† of $M$.

For $n > 1$, the sets $H(N)$ are subcontinua of $M$ (hitherto unknown) which are not disconnected by the omission of any $n$ points and are maximal with respect to this property. For example, for $n = 4$, let $C_1$ and $C_2$ be concentric circles of radii 1 and 2, respectively; let $Q$ be a square, together with its interior, inscribed in $C_1$, let $I$ be the annular region between $C_1$ and $C_2$, and let $M = C_1 + C_2 + I + Q$. Then $M$ has two sets $H(N)$, namely, $C_1 + C_2 + I$ and $Q$; and it will be noted that, conforming to §3,

* See my paper, American Journal of Mathematics, vol. 55 (1933), p. 456.

† See American Journal of Mathematics, vol. 50 (1928), pp. 167–194.

their common part contains just four points and hence is a $T$-set. The situation is exactly the same in this example for any $n>4$.

(iii) Let $T$ be the property of being countable (that is, of power $\leqq \aleph_0$).

As an example, let $C_1$, $C_2$, and $I$ be defined as under (ii), let $J$ be any simple closed curve having any countable set of points in common with $C_1$ and lying otherwise within $C_1$, let $D$ be the interior of $J$ and let $M=C_1+C_2+I+D$. Then the sets $C_1+C_2+I$ and $J+D$ are the sets $H(N)$ in $M$.

(iv) Let $T$ be the property of being homeomorphic with some proper subset of a simple closed curve.

As an example for this case, let $S$ denote the surface of the unit sphere in $R_3$ and let $M$ be $S$+any one-dimensional structure which together with $S$ forms a continuum, for example, the part of the $x$, $y$, and $z$ axes lying within $S$. Then $S$ is the only set $H(N)$ in $M$.

(v) Let $T$ be the property of being at most $(n-2)$-dimensional, $(n=2, 3, 4, \cdots)$.

In this case the sets $H(N)$ are the so-called "$n$-dimensional components"* or the "maximal $n$-dimensional cantorian manifolds"† in $M$. In this case also it will be noticed that §3 above gives the known fact that the common part of any two $n$-dimensional components is at most $(n-2)$-dimensional.

(vi) Let $T$ be the property of being the carrier of no essential complete $n$-dimensional cycle,‡ $(n=0, 1, 2, \cdots)$. (We shall consider only non-oriented cycles.)

For $n=0$, we have identically the case $n=1$ considered under (ii), since any set containing more than one point is the carrier of a 0-cycle.§ Thus in case $M$ is a locally connected continuum, we obtain the true cyclic elements of $M$ for the sets $H(N)$.

For $n=1$, let us consider the following example. Let $W$ denote the set consisting of the surface of a torus together with a coaxial disc just fitting into it, (that is, a disc-wheel with tire attached), and let $C$ be the surface of a cube which is attached

* See Alexandroff, Mathematische Annalen, vol. 106 (1932), p. 215.

† Tumarkin, Comptes Rendus, vol. 186 (1928), p. 420.

‡ See Vietoris, Mathematische Annalen, vol. 97 (1927), p. 458; Alexandroff, Annals of Mathematics, (2), vol. 30 (1928), p. 159.

§ We consider a 0-cycle as any *even number* of points (0-cells).

to $W$ along some simple arc, and let $Q$ be a 2-cell (topological square plus its interior) attached to $C$ along some arc and having nothing in common with $W$. Then $W$ and $C$ are the sets $H(N)$ for $W+C+Q$.

In general, for any $n$, examples indicate that in this case the sets $H(N)$ are maximal subcontinua without *edge points*; and in many ways they seem to be true generalizations of the cyclic elements of locally connected continua (to which they reduce in case $n=0$) and hence might well be called the "$n$th order cyclic elements"* of $M$. We shall consider these sets further in the next section.

5. *Cyclic Elements of nth Order.* Throughout this section we shall let $T$ be the property considered under (vi) in §4 of being the carrier of no essential complete $n$-cycle, and we shall suppose $M$ to be compact. We shall show that in this case the sets $H(N)$ in a compact continuum $M$ have the property that if $K$ is any subcontinuum of $M$ such that every $n$-cycle in $K$ is $\sim 0$ in $K$, then every $n$-cycle in $K \cdot H(N)$ is $\sim 0$ in $K \cdot H(N)$.

For $n=0$ this gives simply the known fact† that the product of any subcontinuum of $M$ by any set $H(N)$ is either vacuous or connected; and in case $M$ is locally connected, it is a special case of the well known and useful property of cyclic elements that the product of any cyclic element by an arbitrary connected set in $M$ is either vacuous or connected.

Now this result is an immediate consequence of the following somewhat sharper theorem.

THEOREM. *If $C$ is an irreducible carrier of the $n$-dimensional complete cycle $C^n$ in $H(N)$ and $B$ is any irreducible membrane‡ in $M$ which is a carrier of the homology $C^n \sim 0$, then we have $B \subset H(N)$.*

For $n=0$ this says simply that every irreducible continuum in $M$ between two points of $H(N)$ is contained in $H(N)$, a known result (see my paper, loc. cit.). We shall prove the theorem with the aid of the following lemma.

LEMMA. *If $C$ is any carrier of an $n$-cycle $C^n$, if $B$ is an irreducible membrane in $M$ which carries the homology $C^n \sim 0$, and $T$ is*

* See R. L. Wilder, this Bulletin, vol. 38 (1932), p. 678.

† See my papers cited above.

‡ See Alexandroff, loc. cit., p. 179.

*any T-set (that is, a set carrying no essential n-cycle) disconnecting B, then for every separation $B-T=B_1+B_2$ we have $B_1 \cdot C \neq 0 \neq B_2 \cdot C$.*

PROOF OF THE LEMMA. Suppose, on the contrary, that for some such separation we have $B_2 \cdot C = 0$. Then we shall show that $B_1+T$ carries the homology $C^n \sim 0$ so that $B$ is reducible. Now we have $C^n = (z_1, z_2, \cdots)$, and since $C^n \sim 0$ in $B$, then $z_i$ bounds a $\delta_i$-complex $K_i^{n+1}$ in $B$ and $\lim \delta_i = 0$. For each $i$, let $H_i^{n+1}$ be the complex consisting of all simplexes of $K_i^{n+1}$ which have all their vertices in $B_1+T$, and let $c_i$ be the boundary of the complementary complex of $H_i^{n+1}$ in $K_i^{n+1}$. Let us now replace $c_i$ by an $n$-cycle $c_i^*$ in $T$ as follows. For each vertex $x_i$ of $c_i$, let us take a point $x_i^*$ in $T$ such that $\rho(x_i, x_i^*) = \rho(x_i, T)$, that is, a point of $T$ which is as near $x$ as any point of $T$. For each simplex $(x_0, x_1, \cdots, x_n)$ of $c_i$, let $(x_0^*, x_1^*, \cdots, x_n^*)$ be a simplex. Then the complex $c_i^*$ of all such simplexes is an $n$-cycle in $T$. Let $\epsilon_i^*$ be the norm of $c_i^*$, that is, the maximum of the diameters of the simplexes of $c_i^*$.

Now since each simplex of $c_i$ is on a $\delta_i$-simplex of $K_i^{n+1}$ which has at least one vertex in $B_2$, it follows that if $d_i = \max \rho(x_i, x_i^*)$, then $\lim d_i = 0$. Thus since $\delta_i \to 0$, it follows that $\epsilon_i^* \to 0$. Now if $\delta_i'$ is the greatest lower bound of the numbers $\delta$ such that $c_i^*$ bounds a $\delta$-complex in $T$, then since $T$ carries no essential $n$-cycle, it follows by a result of Vietoris† that $\lim \delta_i' = 0$.

Let $\delta_i^* = 2\delta_i'$. Then for each $i$, $c_i^*$ bounds a $\delta_i^*$-complex $L_i^{n+1}$ in $T$ and $\lim \delta_i^* = 0$. Then‡ $L_i^{n+1}+H_i^{n+1}$ is a $(\delta_i+2d_i+\delta_i^*)$-complex bounded by $z_i$ (mod 2), and this complex is contained in $B_1+T$. Thus $C^n \sim 0$ in $B_1+T$, contrary to the fact that $B$ is irreducible; and our lemma is established.

PROOF OF THE THEOREM. We have only to show that $H(N)+B$ is not disconnected by the omission of any $T$-set. Suppose, on the contrary, that for some $T$-set $T$, we have a separation $H(N)+B-T=H_1+H_2$. Then since $H(N)-T \cdot H(N)$ is connected, it must be contained wholly in either $H_1$ or $H_2$, say $H_1$. Thus $C-C \cdot T \subset H_1$ and $H_2 \subset B-C$. But we have the separation

† See Vietoris, loc. cit., p. 464.

‡ It is understood that we take here the modified complex $H_i^{n+1}$, that is, the one obtained after replacing each $x_i$ in $c_i$ by the corresponding $x_i^*$.

$B-B\cdot T=H_2+H_1\cdot B$, and $H_2\cdot C=0$, contrary to the lemma.

6. *Conclusion.* In conclusion attention is called to the desirability of clearing up, in the general case, the possibilities for the power of the class of all sets $[H(N)]$ in a compact space for any system $T$, such as has already been done by Mazurkiewicz and Alexandroff (see papers in Fundamenta Mathematicae, vols. 19 and 20) in the special case of the dimensional components. Also a more detailed study of the structure of continua $M$ of varying degrees of connectivity and local connectivity with respect to the sets $H(N)$, in particular in the case* considered in §5, would be highly desirable.

THE JOHNS HOPKINS UNIVERSITY

## INTEGRAL DOMAINS OF RATIONAL GENERALIZED QUATERNION ALGEBRAS†

BY A. A. ALBERT

1. *Introduction.* We shall consider generalized quaternion algebras

$$Q = (1, i, j, ij), \qquad ji = -ij, \qquad i^2 = \alpha, \qquad j^2 = \beta,$$

over the field $R$ of all rational numbers. It is easily shown that, by a trivial transformation on the basis of $Q$, we may take $\alpha$ and $\beta$ to be integers without square factors.

Of great interest in the theory of algebras $Q$ are the integral sets of $Q$. L. E. Dickson‡ has called a set $S$ of quantities of $Q$ an integral set if $S$ satisfies the following postulates:

$R$: The quantities of $S$ have minimum equations with ordinary whole number coefficients and leading coefficient unity.

$C$: $S$ is closed under addition, subtraction, and multiplication.

$U$: $S$ contains $1, i, j$.

$M$: $S$ is maximal.

---

* A further study of this case is made in the author's paper *Cyclic elements of higher order*, to appear in the American Journal of Mathematics, vol. 56 (1934).

† Presented to the Society, June 19, 1933.

‡ See Dickson's *Algebren und ihre Zahlentheorie*, pp. 154–197, for his theory as well as references to the work of Latimer and Darkow. See also Latimer's later paper, Transactions of this Society, vol. 32 (1930), pp. 832–846.

Using the above definition for $S$, Dickson considered the integral sets for algebras $Q$ with $\alpha=-1$. By a further transformation on the basis of algebras $Q$, Dickson showed, for his case $\alpha=-1$, that $\beta$ could be taken to have no prime factors $p=4n+1$. He then obtained the sets $S$. Latimer considered algebras $Q$ with $\alpha\equiv\beta\equiv 1 \pmod 2$, and with $\alpha\equiv 2$, $\beta\equiv 1 \pmod 8$ and, after transformations on the basis of $Q$, obtained many sets $S$ for each algebra $Q$. Similar considerations were made by Marguerite Darkow for the case $\alpha\equiv\beta\equiv 2 \pmod 4$. These latter results of Latimer and Darkow are very complicated and do not *complete* the problem of finding an integral set for every generalized quaternion algebra.

The above division into special cases is certainly not desirable. Nor is it necessary. For it is obvious that at least an attempt should be made to show that transformations carrying all the cases into a canonical form are possible and it is this canonical form which should be studied.

In the present paper such a canonical form is obtained. It is shown that every rational generalized quaternion algebra is equivalent to an algebra with $\alpha=\tau\equiv 1 \pmod 4$, where $-\tau$ is a positive prime. The integer $\beta=\sigma$ is also restricted. In particular it is evident that integral sets $S$ should contain the integers of the field $R(i)$ and hence 1, $P=(1+i)/2$, is a basis of such integers. Hence the postulate $U$ is replaced here by

$U'$: $S$ contains 1, $P$, $j$.

But then it is shown that there exist two* sets $S$, $\overline{S}$ satisfying $R$, $C$, $U'$, $M$, and the bases of these sets are explicitly determined.

2. *Transformations on Algebras $Q$.* Let $R$ be the field of all rational numbers and let $Q$ be any normal simple algebra of degree two over $R$. Then

$$(1)\quad Q = Q(\alpha,\beta) = (1, i, j, ij),\quad ji = -ij,\quad i^2=\alpha,\quad j^2=\beta,$$

where $\alpha\neq 0$ and $\beta\neq 0$ are in $R$. Conversely, every algebra (1) is normal simple.

* Essentially only one set, as we show here that $\sigma=\epsilon\tau+4\mu^2$ and obtain a corresponding set $S$. But then $\sigma=\epsilon\tau+4(-\mu)^2$ and $\overline{S}$ is obtained from $S$ by replacing $\mu$ by $-\mu$.

If we have $i_0=\lambda i$, $j_0=(\lambda+\nu i)j$, then $j_0i_0=-i_0j_0$, $i_0^2=\lambda^2\alpha$, $j_0^2=(\mu^2-a\nu^2)\beta$, and $Q=(1, i_0, j_0, i_0j_0)$. Hence we have the following lemma.

LEMMA 1. *If $\lambda, \mu, \nu$ are rational numbers, then $Q(\alpha, \beta)=Q(\gamma, \delta)$, where $\gamma=\lambda^2\alpha$, $\delta=(\mu^2-\alpha\nu^2)\beta$.*

Next let $i_0=x_1i+x_2j+x_3ij$, so that

$$(2) \qquad i_0^2 = \gamma = f(x_1, x_2, x_3) = x_1^2\alpha + x_2^2\beta - x_3^2\alpha\beta.$$

Then I have proved* the following fact.

LEMMA 2. *If $\gamma=f(x_1, x_2, x_3)\not\equiv x_1^2\alpha$ of (2) for rational $x_1, x_2, x_3$, then $Q(\alpha, \beta)=Q(\gamma, \delta)$, where in fact $\delta=-\alpha\beta(x_2^2-x_3^2\alpha)$.*

If $\alpha$ is rational, then $\alpha=\rho\epsilon^{-1}$, where $\rho$ and $\epsilon$ are relatively prime integers. Then $\rho\epsilon=\xi^2\alpha_0$, where $\xi$ and $\alpha_0$ are integers and $\alpha_0$ has no square factors. If $\alpha_1=\xi\epsilon^{-1}$, then $\alpha=\alpha_1^2\alpha_0$ and we call $\alpha_0$ the *kernel* of $\alpha$.

By Lemma 2 any integer having the form $x_1^2\alpha+x_2^2\beta-x_3^2\alpha\beta$ for rational $x_1, x_2, x_3$ may be chosen as a new $\alpha$. Let $\alpha_0, \beta_0, \gamma_0$ be the kernels of $\alpha, \beta, -\alpha\beta$, respectively, so that every value of the form $F(x, y, z)=\alpha_0x^2+\beta_0y^2+\gamma_0z^2$ for integral $x, y, z$ is represented *rationally* by (2) and may be taken to replace $\alpha$.

Evidently $\gamma_0$ is the kernel of $-\alpha_0\beta_0$, so that not all three of $\alpha_0, \beta_0, \gamma_0$ are even. Moreover, one of $\alpha_0, \beta_0, \gamma_0$ is negative. Either $\alpha_0\equiv\beta_0\equiv\gamma_0\equiv 3 \pmod 4$, so that $F(1, 1, 1)\equiv 9\equiv 1 \pmod 4$, or one letter, say $a$, is even, and one, say $b$, satisfies the congruence $b\equiv 3 \pmod 4$, whence $a\cdot 1^2+b\cdot 1^2\equiv 2+3\equiv 1 \pmod 4$.

If $\alpha>0$, then one of $\beta_0$ and $\gamma_0$, say $b$, is negative, so that $\rho=\alpha+4b\alpha^2=\alpha(1+4\alpha\beta)<0$, $\rho\equiv 1 \pmod 4$, and is a value of $f(x_1, x_2, x_3)$. Hence we may take $\alpha<0$, $\alpha\equiv 1 \pmod 4$.

Let us now apply Lemma 1 to replace $\alpha=\alpha_1^2\alpha_0$, $\beta=\beta_1^2\beta_0$ by their kernels $\alpha_0, \beta_0$. This is evidently accomplished when we have $\lambda=\alpha_1^{-1}$, $\mu=\beta_1^{-1}$, $\nu=0$. Hence take $\alpha_0\equiv 1 \pmod 4$, $\alpha_0<0$.

Let $\pi$ be the greatest common divisor of $\alpha_0, \beta_0$, so that $\alpha_0=\alpha_2\pi$, $\beta_0=\beta_2\pi$. Then $\alpha_2, \beta_2, \pi$ are relatively prime in pairs since $\alpha_0$ and $\beta_0$ have no square factors. It follows that $\alpha_0$ is prime to $\beta_2(\pi-\alpha_2)$. But if $\lambda=1, \mu=1, \nu=\pi^{-1}$ in Lemma 1, then

* See my paper in this Bulletin, vol. 37 (1933), pp. 257–258, for the results implying Lemmas 1 and 2.

$\gamma=\alpha_0$, $\delta=(1-\pi^{-2}\alpha_2\pi)\pi\beta_2=\beta_2/(\pi-\alpha_2)$. We use Lemma 1 to replace $\beta_2(\pi-\alpha_2)$ by its kernel and thus prove the following theorem.

THEOREM 1. *Every normal simple algebra of degree two over $R$ is equivalent to an algebra $Q(\alpha, \beta)$, where $\alpha$ and $\beta$ are relatively prime integers without square factors, $\alpha<0$, $\alpha\equiv 1 \pmod 4$.*

The quadratic form $\phi=-\alpha x^2-4\beta y^2$ has relatively prime coefficients, positive leading coefficient, and discriminant $\Delta=-16\alpha\beta$. Evidently $\Delta$ is an integral square if and only if $-\alpha\beta=1$, $-\alpha=\beta=1$, which is impossible since $-\alpha\equiv 3 \pmod 4$. By the Dirichlet Theorem,* $\phi$ represents infinitely many positive primes $p$. Since $-\alpha\beta$ has only a finite number of prime divisors, infinitely many positive primes $p$ represented by $\phi$ are prime to $-\alpha\beta$. If $\tau=-p$, then

$$\tau = \alpha x^2 + 4\beta y^2, \qquad -\alpha\beta x^2 \equiv (2\beta y)^2 \pmod{\tau}.$$

If $x\equiv 0 \pmod\tau$, then necessarily $y\equiv 0 \pmod\tau$, so that $\alpha x^2+4\beta y^2=\tau\equiv 0 \pmod{\tau^2}$, which is impossible. Hence $x$ is prime to $\tau$, $tx\equiv 1 \pmod\tau$ for integral $t$, $-\alpha\beta\equiv(2\beta yt)^2 \pmod\tau$, and $-\alpha\beta=4\mu^2+\epsilon\tau$ for integral $\mu$, $\epsilon$. By Lemma 2, with $x_1=x$, $x_2=y$, $x_3=0$, we have $\delta=-4\alpha\beta x_2^2$ whose kernel is $-\alpha\beta$. Hence the following theorem is established.

THEOREM 2. *Every normal simple algebra of degree 2 over $R$ is equivalent to an algebra $Q(\tau, \sigma)$, where $\sigma$ has no square factors and is prime to $\tau$, $-\tau$ is a prime, and $\sigma = 4\mu^2 + \epsilon\tau$ when $\tau < 0$ and $\tau \equiv 1 \pmod 4$, for integral $\mu$, $\epsilon$.*

3. *The Removal of Certain Factors of $\sigma$.* It is well known that the quadratic form

$$x^2 - \tau y^2 - \rho z^2, \qquad (\tau, \rho) = 1, \tag{3}$$

is a zero form, for $\tau$ prime to $\rho$, if and only if $\tau$ is a quadratic residue of $\rho$ and $\rho$ is a quadratic residue of $\tau$.

Evidently $\tau$ is a quadratic residue of 2. But 2 is a quadratic residue of $\tau$ if and only if $\tau\equiv 1 \pmod 8$. For if $\tau=-t$, $t$ a prime, then

* See A. Meyer, Journal für Mathematik, vol. 103 (1888), pp. 98–116.

$$(4)\quad \begin{cases} (2\,|\,\tau) = (2\,|\,t) = (-1)^{(t^2-1)/8} = 1, \quad t^2 \equiv \tau^2 \equiv 1 \pmod{16}, \\ (4n+1)^2 \equiv 8n+1 \equiv 1 \pmod{16}, \ n \equiv 0 \pmod 2, \\ \tau = 8n_1 + 1. \end{cases}$$

Let $\rho$ be the product of all the odd prime factors $q$ of $\sigma$ such that $\tau$ is a quadratic residue of each such $q$. Let $\rho_0 = 2\rho$ if $\tau \equiv 1 \pmod 8$ and $\sigma$ is even, while $\rho_0 = \rho$ if either $\sigma$ is odd or $\tau \not\equiv 1 \pmod 8$. Then $x^2 - \tau y^2 - \rho_0 z^2 = 0$ for integral $x, y, z$ not all zero. For $\tau$ is a quadratic residue of $\rho_0$, and $\rho_0$ is a quadratic residue of $\tau$ if and only if $(\rho\,|\,\tau) = 1$, since $-\tau = t$ is a prime.* But

$$(\rho\,|\,\tau) = (\rho\,|\,t) = (-1)^e (t\,|\,\rho) = (-1)^f (\tau\,|\,\rho) = (-1)^f = 1,$$

$$(5)\quad e = \frac{\rho-1}{2}\cdot\frac{t-1}{2}, \qquad f = e + \frac{\rho-1}{2} = \frac{\rho-1}{2}\cdot\frac{t+1}{2},$$

since $(\tau\,|\,\rho) = 1$, $t+1 = -\tau+1 \equiv -1+1 \equiv 0 \pmod 4$.

The integer $z \neq 0$, since $x^2 - y^2\tau$ is not a zero form when $-\tau > 1$, is a prime. Hence $\rho_0 = \lambda^2 - \nu^2\tau$ for rational $\lambda, \nu$. Moreover $\rho_0 = \eta^2 \pmod \tau$, where $\eta$ is prime to $\tau$. Hence $\eta\zeta \equiv 1 \pmod \tau$ for integral $\zeta$, so that, if $\sigma = \sigma_0\rho_0$, then $\rho_0\sigma_0 \equiv 4\mu^2 \pmod \tau$, $\sigma_0 \equiv 4(\mu\zeta)^2 \pmod \tau$. But $Q(\tau,\sigma) = Q(\tau, \sigma_0)$ by Lemma 1 and the following fact is proved.

THEOREM 3. *In Theorem 2 we may take $\tau$ a quadratic non-residue of every odd prime factor of $\sigma$ and $\sigma$ odd if $\tau \equiv 1 \pmod 8$.*

It is well known that $Q(\tau, \sigma)$ is a division algebra if and only if the form

$$(6)\quad x_1^2 - \tau x_2^2 - \sigma x_3^2$$

is not a zero form. Evidently if (6) is a zero form, then $\sigma > 0$. But necessarily if (6) is a zero form, then $\tau$ is a quadratic residue of $\sigma$. Since $\tau$ is a quadratic non-residue of every odd prime factor of $\sigma$, then $\sigma = 1, 2$. If $\sigma = 2$, then (6) implies that 2 is a quadratic residue of $\tau$, so that $\tau \equiv 1 \pmod 8$, a contradiction of Theorem 3. Hence $\sigma = 1$. Conversely, if $\sigma = 1$, then $(j-1)(j+1) = 0$ and $Q$ is not a division algebra.

THEOREM 4. *The algebras of Theorem 3 are all division algebras except for $\sigma = 1$.*

* For of course $\tau$ is already a quadratic residue of $\rho_0$ and $(2\,|\,\tau) = 1$ in the case where $\rho_0$ is even; whence $\tau \equiv 1 \pmod 8$.

Consider now the congruence $x^2\sigma+y^2\tau-z^2\equiv 0 \pmod{4\sigma}$. Then $y^2\tau-z^2\equiv 0 \pmod{\sigma}$. If $q$ is any odd prime factor of $\sigma$ not dividing $y$, then $\tau$ is a quadratic residue of $q$, a contradiction. But $\sigma$ has no square factors so that $\sigma=\sigma_0$ or $2\sigma_0$, where $\sigma_0$ is odd, $y\equiv 0 \pmod{\sigma_0}$ so that $z\equiv 0 \pmod{\sigma_0}$. If $\sigma_1$ is even, then $\tau\not\equiv 1 \pmod 8$, $x^2\sigma+y^2\tau-z^2\equiv 0 \pmod 8$. But $y^2\tau-z^2\equiv 0 \pmod 2$, since $\sigma$ is even. Hence $y\equiv z \pmod 2$ so that, since $\tau\equiv 1 \pmod 4$, we shall have $y^2\tau-z^2\equiv 0 \pmod 4$, $x^2\sigma\equiv 0 \pmod 4$, $x\equiv 0 \pmod 2$, $x^2\sigma\equiv 0 \pmod 8$, and $y^2\tau\equiv z^2 \pmod 8$. If $y$ is odd, then $z$ is odd and $y^2\tau-z^2\equiv\tau-1\equiv 0 \pmod 8$, which is a contradiction. Hence $y$ is even, $y\equiv z\equiv 0 \pmod 2$, and we have proved the following result.

THEOREM 5. *The integral congruence* $x^2\sigma+y^2\tau-z^2\equiv 0 \pmod{4\sigma}$ *implies that* $y\equiv z\equiv 0 \pmod{\sigma}$.

4. *On Domains of Integrity.* Let $D$ be a rational semi-simple algebra of order $n$. A set $S$ of quantities of $D$ is called a domain of integrity if it is closed under addition, subtraction, multiplication. Assume also that the quantities of $S$ satisfy integral equations and that $S$ contains the modulus 1 of $D$. Then if $S$ has order $n$, it is well known* that $S$ has a basis

$$\omega_{10}, \omega_{20}, \cdots, \omega_{n0} = 1. \tag{7}$$

We may evidently write

$$\omega_{i0} = \sum_{j=1}^{n} \alpha_{ij} u_{j0}, \qquad (i = 1, \cdots, n),$$

where the $u_{j0}$ are a basis of $D$, the $\alpha_{ij}$ are rational, and

$$u_{n0} = 1. \tag{8}$$

Then the matrix $A=\|\alpha_{ij}\|$ is non-singular and

$$A = \alpha^{-1}\|\beta_{ij}\| = \alpha^{-1}B, \tag{9}$$

where $B$ is an integer matrix, $\alpha$ is an integer. If $C=\|c_{ij}\|$ is an integer matrix of determinant unity, the transformation

$$\omega_{i0}' = \sum c_{ij}\omega_{i0} \tag{10}$$

evidently replaces the $\omega_{j0}$ by a new basis of $S$. But it is well

* See Dickson, *Algebren und ihre Zahlentheorie*, p. 212.

known† that there exists such a matrix $C$ such that

$$CB = B_0 = \|\gamma_{ij}\| \tag{11}$$

has elements below the diagonal all zero. Then

$$\omega_i' = \alpha^{-1} \sum \gamma_{ij} u_{j0} = \sum \delta_{ij} u_{j0}. \tag{12}$$

But now re-arrange the $u_{i0}$ so that $u_i = u_{n-i,0}$ and similarly $\omega_i = \omega_n'_{-i}$. Then

$$\omega_i = \sum_{j=1}^{i} a_{ij} u_j, \tag{13}$$

with rational $a_{ij}$. In particular

$$\omega_1 = a_{11} \cdot 1, \qquad (a_{11} \text{ in } R), \tag{14}$$

satisfies an integral equation so that $a_{11}$ is integral. But unity is in $S$ so that, since each $\omega_i$ contains one more basal unit than $\omega_{i-1}$, we evidently must have unity an integral multiple of $\omega_1$. Hence $a_{11} = 1$.

THEOREM 6. *If $D$ is a rational semi-simple algebra of order $n$ and $S$ is a domain of integrity of the $n$th order in $D$ such that the quantities of $S$ satisfy integral equations and the modulus $u_1 = 1$ of $A$ is in $S$, then $S$ has a basis*

$$\omega_i = \sum_{j=1}^{i} a_{ij} u_j, \qquad (\omega_1 = 1, \, a_{ij} \text{ in } R), \tag{15}$$

*for $i = 1, \cdots, n$.*

In particular let $S$ contain the basal quantities of $D$. Then

$$u_i = \sum_{j=1}^{n} \eta_{ij} \omega_j, \qquad (i = 1, \cdots, n), \tag{16}$$

with integer $\eta_{ij}$. Since the $u_i$ are linearly independent in $R$, and $\omega_n$ contains $u_n$, but no other $\omega_i$, $(i < n)$, contains $u_n$, we evidently have $\eta_{in} = 0$, $(i < n)$. Similarly $\eta_{ij} = 0$, $(j = i+1, \cdots, n)$, so that

$$u_i = \sum_{j=1}^{i-1} \eta_{ij} \omega_j + \eta_{ii} \omega_i.$$

† Ibid., p. 221.

Again applying the linear independence of the $u_i$ to coefficients of the $u_i$, we have

$$1 = a_{ii}\eta_{ii}, \tag{17}$$

so that we have proved the following theorem.

THEOREM 7. *If $S$ contains the basal quantities of $A$ and if* (15) *holds we have*

$$a_{ii} = \frac{1}{\alpha_{ii}}, \tag{18}$$

*where the $\alpha_{ii}$ are integral.**

Let us consider now a generalized quaternion algebra

$$Q = (1, i, j, ij), \qquad ji = -ij, \qquad i^2 = \tau, \qquad j^2 = \sigma, \tag{19}$$

with integer $\tau$ and $\sigma$. Then if $S$ is a domain of integrity of $Q$ which contains the quantities $1, i, j$, and hence $ij$, and which is such that the quantities of $S$ satisfy integral equations, then $S$ has a basis

$$\begin{aligned} &\omega_1 = 1, && \omega_3 = \beta_1 + \beta_2 i + \beta_3 j, \\ &\omega_2 = \alpha_1 + \alpha_2 i, && \omega_4 = \gamma_1 + \gamma_2 i + \gamma_3 j + \gamma_4 ij, \end{aligned} \tag{20}$$

with rational $\alpha_i$, $\beta_i$, $\gamma_i$. Every quantity

$$x = \delta_1 + \delta_2 i + \delta_3 j + \delta_4 ij \tag{21}$$

satisfies

$$\omega^2 - 2\delta_1\omega + N(x) = 0, \tag{22}$$

where $x$ satisfies an integral equation only for integer

$$2\delta_1, \qquad N(x) = \delta_1^2 - \delta_2^2\tau - \delta_3^2\sigma + \delta_4^2\tau\sigma. \tag{23}$$

Hence $2\alpha_1$, $2\beta_1$, $2\gamma_1$, are rational integers. Also $i\omega_2 = \alpha_2\tau + \alpha_1 i$

---

* Notice that in fact

$$\omega_i = \alpha_{ii}^{-1}\Big(u_i - \sum_{j=1}^{i-1}\alpha_j\omega_j\Big)$$

which may simplify the determination of $\omega_i$ after the $\omega_j$ are determined. This fact is not used here.

satisfies an integral equation (22), so that $2\alpha_2\tau$ is integral. Similarly $2\beta_2\tau$, $2\beta_3\sigma$, $2\gamma_2\tau$, $2\gamma_3\sigma$, $2\gamma_4\sigma\tau$ are integers. But $\alpha_2$, $\beta_3$, $\gamma_4$ are the reciprocals of integers by Theorem 6. Hence we have proved the following theorem.

THEOREM 8. *Let $Q$ be a generalized quaternion algebra* (19) *over $R$ and let $S$ be a domain of integrity of $Q$ containing* $1, i, j, ij$, *and with all its quantities satisfying integral equations. Then $S$ has a basis*

$$(24)\quad \begin{cases} \omega_1 = 1, \quad \omega_2 = \dfrac{\xi_1}{2} + \dfrac{1}{\xi_2}\, i, \quad \omega_3 = \dfrac{\eta_1}{2} + \dfrac{\eta_2}{2\tau}\, i + \dfrac{1}{\eta_3}\, j, \\ \omega_4 = \dfrac{\zeta_1}{2} + \dfrac{\zeta_2}{2\tau}\, i + \dfrac{\zeta_3}{2\sigma}\, j + \dfrac{1}{\zeta_4}\, ij, \end{cases}$$

*where the $\xi_i$, $\eta_i$, $\zeta_i$ are integers, and*

$$(25)\quad 2\tau \equiv 0 \pmod{\xi_2}, \quad 2\sigma \equiv 0 \pmod{\eta_3}, \quad 2\sigma\tau \equiv 0 \pmod{\zeta_4}.$$

5. *Two Integral Sets of $Q$.* We shall consider generalized quaternion division algebras $Q$ over $R$. Our algebras are therefore algebras of Theorem 4 with $\sigma \neq 1$. Consider the quantities

$$(26)\quad v_1 = 1, \quad v_2 = \frac{1+i}{2}, \quad v_3 = j, \quad v_4 = \frac{i(2\mu + j) + \tau j}{2\tau}.$$

Since $\tau = 4n+1$, $\sigma = 4\mu^2 + \epsilon\tau$, we have

$$(27)\quad v_3^2 = \sigma, \quad v_2^2 = v_2 + n, \quad v_4^2 = \epsilon n + \mu^2,$$

so that the quantities (26) satisfy integral equations.

We study the set $S$ of linear combinations

$$(28)\quad \sum_{i=1}^{n} \lambda_i v_i$$

with integer $\lambda_i$. Evidently $S$ satisfies $U'$, since $S$ contains $1$, $P = v_2, j$. Also $S$ is closed under addition and subtraction. It is evident that, since the basal quantities (26) of $S$ satisfy integral equations, $S$ will satisfy postulates $R$ and $C$ if and only if $S$ is closed under multiplication. In order to prove this closure we need only prove that $S$ contains

$$v_2v_3, \quad v_3v_2, \quad v_2v_4, \quad v_4v_2, \quad v_3v_4, \quad v_4v_3. \tag{29}$$

In particular $S$ contains

$$j = v_2, \quad i = 2v_2 - 1, \quad ij = 2\tau v_4 - 2\mu i - \tau j. \tag{30}$$

We compute

$$v_3v_2 = \frac{j(i+1)}{2} = \frac{(1-i)j}{2} = (1 - v_2)v_3 = v_3 - v_2v_3, \tag{31}$$

which is in $S$ if and only if $v_2v_3$ is in $S$. But

$$v_2v_3 = \frac{(1+i)}{2} j = \tau v_4 - \mu i - 2\eta j \tag{32}$$

is in $S$. Also

$$\begin{cases} v_4v_3 = \dfrac{i(2\mu j + \sigma) + \sigma\tau}{2\tau} = 2\mu v_4 + \dfrac{\sigma - 4\mu^2}{2\tau} i - \mu j + \dfrac{\sigma}{2} \\ \quad = 2\mu v_4 - \mu v_3 + \dfrac{\lambda i + \sigma}{2} \\ \quad = 2\mu v_4 - \mu v_3 + 2n\epsilon + \epsilon\left(\dfrac{1+i}{2}\right) \\ \quad = 2(\mu^2 + n\epsilon) + \epsilon v_2 - \mu v_3 + 2\mu v_4 \end{cases} \tag{33}$$

is in $S$, while

$$v_3v_4 + v_4v_3 = \sigma, \tag{34}$$

so that $v_3v_4$ is in $S$.

It remains to prove $v_2v_4$ and $v_4v_2$ in $S$. Now

$$v_2v_4 = \frac{1+i}{2} \frac{2\mu i + ij + \tau j}{2\tau} = \frac{2\mu\tau + 2\mu i + 2\tau j + (\tau + 1)ij}{4\tau}. \tag{35}$$

Since

$$\frac{ij}{2\tau} = v_4 - \frac{2\mu i + \tau j}{2\tau}, \tag{36}$$

we have

$$(37)\quad \begin{cases} v_2v_4 = \dfrac{\tau+1}{2}v_4 + \dfrac{2\tau j + 2\mu i + 2\mu\tau - (\tau+1)(2\mu i + \tau j)}{4\tau} \\ \quad = (2n+1)v_4 + \dfrac{\tau(1-\tau)j + 2\mu\tau(1-i)}{4\tau} \\ \quad = (2n+1)v_4 - nv_3 + \mu v_2 - \mu \end{cases}$$

in $S$. Finally

$$(38)\quad \begin{cases} v_2v_4 + v_4v_2 = v_2v_4 + \dfrac{2\mu\tau + 2\mu i + (1-\tau)ij}{4\tau} \\ \quad = \mu + \dfrac{4\mu i + 2\tau j + 2ij}{4\tau} = \mu + v_4 \end{cases}$$

is in $S$, so that $v_4v_2$ is in $S$. We have therefore proved that $S$ satisfies properties $R$, $C$, $U'$.

Since $\sigma = 4\mu^2 + \epsilon\tau$, we have also $\sigma = 4(-\mu)^2 + \epsilon\tau$, so that our above argument by which we proved that $S$ has properties $R$, $C$, $U'$ also proves that the set $\overline{S}$ with basis

$$(39)\quad y_i = v_i, \qquad (i = 1, 2, 3), \qquad y_4 = \frac{i(-2\mu + j) + j\tau}{2\tau},$$

also has properties $R$, $C$, $U'$. Moreover $S$ and $\overline{S}$ are actually distinct. For otherwise $y_4$ is in $S$, $v_4 + y_4 - j = \tau^{-1}ij$ is in $S$, whence $-\tau^{-2}\sigma\tau = -\sigma\tau^{-1}$ is an integer, contrary to our hypothesis that $\sigma \not\equiv 0 \pmod{\tau}$.

We shall now prove that every set $T$ which satisfies $R$, $C$, $U'$ is either in $S$ or in $\overline{S}$ and hence each of $S$ and $\overline{S}$ is maximal. We will then have proved $S$ and $\overline{S}$ the only sets satisfying $R$, $C$, $U'$, $M$.

Let then $T$ satisfy $R$, $C$, $U'$. Since $T$ is a domain of integrity, it has a basis (24). Hence $\omega_1 = 1$ is in $S$, $\overline{S}$. Also $\omega_2$ is an integer of the algebraic field $R(i)$ and hence, as is well known,* is an integral linear combination of $1$, $v_2$. Hence $\omega_2$ is in $S$, $\overline{S}$.

We next write

$$(40)\qquad \omega_3 = \frac{\eta_1}{2} + \frac{\eta_2 i}{2}\tau + \frac{1}{\eta_3}j, \qquad 2\sigma \equiv 0 \pmod{\eta_3}.$$

* Dickson, loc. cit., p. 149.

But then

$$\omega_3' = \omega_3 - \eta_1 v_2 = \frac{\eta_2 - \eta_1\tau}{2} i + \frac{1}{\eta_3} j$$

is in $T$, since $T$ has property $C$. Hence without loss of generality we may take $\eta_1 = 0$ in (40).

The quantity $\omega_3$ must have an integral minimum equation. This equation evidently is

$$\omega_3^2 = \frac{\eta_2^2\eta_3^2 + 4\sigma\tau}{4\tau\eta_3^2},$$

so that

$$\eta_2^2\eta_3^2 + 4\sigma\tau \equiv 0 \pmod{4\tau\eta_3^2}.$$

Then $4\sigma\tau \equiv 0 \pmod{\eta_3^2}$. Since $\sigma\tau$ has no square factor, we have $4 \equiv 0 \pmod{\eta_3^2}$, $\eta_3 = \pm 1, \pm 2$. But then $\eta_2^2 \equiv 0 \pmod{\tau}$, so that

$$\eta_2 = \eta\tau, \qquad \omega_3 = \frac{\eta i}{2} + \frac{1}{\eta_3} j.$$

Compute

$$v_2\omega_3 = \left(\frac{1+i}{2}\right)\left(\frac{\eta i}{2} + \frac{1}{\eta_3} j\right) = \frac{\eta\tau}{4} + \frac{\eta i}{4} + \frac{j}{2\eta_3} + \frac{ij}{2\eta_3},$$

which must have integral minimum equation (22). Hence $\eta\tau/2$ is an integer, so that $\eta = 2\eta_0$ is even, $\omega_3 - \eta_0 i = \eta_3^{-1} j$ is in $T$ and has integral minimum equation $\omega^2 = \sigma\eta_3^{-2}$. Since $\sigma$ has no square factor, we have $\eta_3 = \pm 1$, and $\omega_3 = \eta_0 i \pm j$ is in $S$, $\bar{S}$ as desired.

We finally consider the quantity $\omega_4$. By the above transformation on $\omega_3$ we may take $\zeta_1 = 0$ in (21) and write

$$\omega_4 = \frac{\zeta_2 i}{2\tau} + \frac{\zeta_3 j}{2\sigma} + \frac{ij}{\zeta_4}, \tag{41}$$

where $2\sigma\tau \equiv 0 \pmod{\zeta_4}$. Then $2\sigma\tau = \zeta_4\zeta_5$ and

$$\omega_4 = \frac{\zeta_2 i}{2\tau} + \frac{\zeta_3 j}{2\sigma} + \frac{\zeta_5 ij}{2\sigma\tau}, \tag{42}$$

so that

$$\omega_4^2 = \frac{\zeta_2^2\tau}{4\tau^2} + \frac{\zeta_3^2\sigma}{4\sigma^2} - \frac{\zeta_5^2\sigma\tau}{4\sigma^2\tau^2} = \frac{\zeta_2^2\sigma + \zeta_3^2\tau - \zeta_5^2}{4\sigma\tau} \tag{43}$$

must be integral.

By Theorem 5 we have $\zeta_3 = x_3\sigma, \zeta_5 = x_5\sigma$, and $\zeta_2^2 + (x_3^2\tau - x_5^2) \equiv 0 \pmod{4\tau}$, which is equivalent to

$$(44) \qquad \zeta_2^2 - x_5^2\sigma \equiv 0 \pmod{\tau}, \quad \zeta_2^2 + x_3^2\tau - x_5^2 \equiv 0 \pmod{4}.$$

Also

$$\omega_4 = \frac{\zeta_2 i}{2\tau} + \frac{x_3 j}{2} + \frac{x_5 ij}{2\tau},$$

so that, since $v_2 = 1 + i/2$ is in $T$, so is

$$v_2\omega_4 = \frac{\zeta_2}{4} + \frac{\zeta_2}{4\tau} i + \frac{x_3 + x_5}{4} j + \frac{x_3\tau + x_5}{4\tau} ij.$$

Since then $v_2\omega_2$ must have integral minimum equation, we see that $\zeta_2/2$ is integral, $\zeta_2^2 \equiv 0 \pmod{4}$, $x_3^2\tau - x_5^2 \equiv 0 \pmod{2}$ and $x_3 \equiv x_5 \pmod{2}$. But then $x_3^2\tau - x_5^2 \equiv 0 \pmod{4}$ and $(44)_2$ is satisfied. We write $x_3 = x_5 + 2\lambda$.

Since $\sigma \equiv 4\mu^2 \pmod{\tau}$, we have $\zeta_2^2 \equiv (2\mu x_5)^2 \pmod{\tau}$. But $-\tau$ is a prime so that $\zeta_2 \equiv \pm 2\mu x_5 \pmod{\tau}$, $\zeta_2 = \pm 2\mu x_5 + y\tau$. Since $\zeta_2$ is even, so is $y = 2z$ and

$$\omega_4 = x_5\left(\frac{\pm 2\mu i + \tau j + ij}{2\tau}\right) + \lambda j + zi,$$

which is evidently in $S$ or $\overline{S}$ according as the above sign is plus or minus. Hence $T$ is contained in $S$ or $\overline{S}$ as desired.

THEOREM 9. *Every generalized quaternion division algebra in its canonical form of Theorem 4 has precisely two sets $S$, $\overline{S}$ of integral quantities satisfying R, C, U', M, and with*

$$\omega_1 = 1, \quad \omega_2 = \frac{1 + i}{2}, \quad \omega_3 = j, \quad \omega_4 = \frac{i(2\mu + j) + \tau j}{2},$$

*as a basis of $S$, while $\overline{S}$ has the corresponding basis*

$$\omega_1 = 1 \quad \omega_2 = \frac{1 + i}{2}, \quad \omega_3 = j, \quad \overline{\omega}_4 = \frac{i(-2\mu + j) + \tau j}{2\tau}.$$

It is evident that the two sets $S$, $\overline{S}$ have almost identical properties and hence that there is essentially one set (either $S$ or $\overline{S}$) of integral quantities of $Q$.

THE INSTITUTE FOR ADVANCED STUDY

## OFFICIAL COMMUNICATIONS

Meetings of the Society have been fixed at the following times and places:

The usual February Meeting in New York City will be omitted.

NEW YORK CITY, March 30-31, 1934.

Abstracts must be in the hands of Associate Secretary J. R. Kline, 501 West 116th St., New York City, not later than March 9. Abstracts received by the Secretaries by that date will appear in the March issue of the BULLETIN. By invitation of the program committee, there will be a symposium on *Algebraic geometry*, under the leadership of Professors A. B. Coble, Solomon Lefschetz, Oscar Zariski, and Virgil Snyder.

CHICAGO, ILLINOIS, April 6-7, 1934.

Abstracts must be in the hands of Associate Secretary M. H. Ingraham, University of Wisconsin, Madison, Wis., not later than March 9. Abstracts received by the Secretaries by that date will appear in the March issue of the BULLETIN. At this meeting, Professor R. E. Langer will give an address on *The asymptotic solutions of linear ordinary differential equations.*

BERKELEY, CALIFORNIA, June 20, 1934.

Abstracts must be in the hands of Associate Secretary T. M. Putnam, University of California, Berkeley, Calif., not later than May 30. Abstracts received by the Secretaries by May 6 will appear in the May issue of the BULLETIN.

WILLIAMSTOWN, MASSACHUSETTS, SUMMER MEETING AND COLLOQUIUM, September 4-7, 1934.

Abstracts must be in the hands of Associate Secretary J. R. Kline, 501 West 116th St., New York City, not later than August 1. Abstracts received by July 6 will appear in the July issue of the BULLETIN. Professor Norbert Wiener will deliver a series of colloquium lectures which were planned by himself and the late Dr. R. E. A. C. Paley on *Topics from harmonic analysis in the complex domain.*

R. G. D. RICHARDSON, *Secretary of the Society.*

---

Articles for insertion in the BULLETIN should be addressed to E. R. HEDRICK, Editor of the BULLETIN, University of California at Los Angeles. Reviews should be sent to W. R. LONGLEY, Yale University, New Haven, Conn. Notes should be sent to H. W. KUHN, Ohio State University, Columbus, Ohio.

Subscriptions to the BULLETIN, orders for back numbers, and inquiries in regard to non-delivery of current numbers should be addressed to the American Mathematical Society, 450-459 Ahnaip St., Menasha, Wis., or 501 West 116th St., New York.

The initiation fees and the annual dues of members of the Society (see this BULLETIN, p. 322, May, 1930; and the List of Officers and Members, September, 1932, p. 66), are payable to the Treasurer of the Society, Professor G. W. Mullins, 501 West 116th St., New York City.

WHOLE NUMBER 413

## CONTENTS


| | PAGE |
|---|---|
| Note on a Problem of Fréchet. By ROTHWELL STEPHENS. | 65 |
| On the Summation of Fourier Series. By R. E. A. C. PALEY, W. C. RANDELS, and M. F. ROSSKOPF. | 69 |
| Curvatures in Riemannian Space. By HARRY LEVY. | 75 |
| A Note on a certain Property of a Family of Curves. By ALBERT WERTHEIMER. | 79 |
| Note on Homogeneous Functionals. By L. S. KENNISON. | 80 |
| Note on the Orthogonality of Tchebycheff Polynomials on Confocal Ellipses. By J. L. WALSH. | 84 |
| Derivatives, Difference Quotients, and Taylor's Formula. By HASSLER WHITNEY. | 89 |
| Linear Associative Algebras of Infinite Order whose Elements satisfy Finite Algebraic Equations. By H. H. CONWELL. | 95 |
| The Apparent Contour of the General $V_3^n$ in $S_4$. By A. R. WILLIAMS. | 103 |
| On Power Characters in Cyclotomic Fields. By H. S. VANDIVER | 111 |
| Fermat's Last Theorem and the Second Factor in the Cyclotomic Class Number. By H. S. VANDIVER. | 118 |
| Independent Postulates for the "Informal" Part of Principia Mathematica. By E. V. HUNTINGTON. | 127 |
| Independent Postulates for an "Informal Principia System with Equality." By E. V. HUNTINGTON. | 137 |
| A Cyclic Involution of Order Seven. By W. R. HUTCHERSON. | 143 |
| Note on Relations connecting certain Cases of Convergence in the Mean. By DUNHAM JACKSON. | 152 |
| Concerning Maximal Sets. By G. T. WHYBURN. | 159 |
| Integral Domains of Rational Generalized Quaternion Algebras. By A. A. ALBERT. | 164 |


---

For Official Communications and Notices, see the inside of the back cover.

GEORGE BANTA PUBLISHING COMPANY, MENASHA, WISCONSIN